

1 Mike Arias (CSB #115385)  
2 Elise R. Sanguinetti (CSB #191389)  
3 Arnold C. Wang (CSB #204431)  
4 Craig S. Momita (CSB #163347)  
5 M. Anthony Jenkins (CSB #171958)  
6 **ARIAS SANGUINETTI WANG & TORRIJOS LLP**  
7 6701 Center Drive West, Suite 1400  
8 Los Angeles, California 90045  
9 Telephone: (310) 844-9696  
10 Facsimile: (310) 861-0168  
11 [mike@aswtlawyers.com](mailto:mike@aswtlawyers.com)  
12 [arnold@aswtlawyers.com](mailto:arnold@aswtlawyers.com)  
13 [craig@aswtlawyers.com](mailto:craig@aswtlawyers.com)  
14 [anthony@aswtlawyers.com](mailto:anthony@aswtlawyers.com)

15 Thomas P. Rosenfeld (*pro hac vice* forthcoming)  
16 Kevin P. Green (*pro hac vice* forthcoming)  
17 Thomas C. Horscroft (*pro hac vice* forthcoming)  
18 **GOLDENBERG HELLER & ANTOGNOLI, P.C.**  
19 2227 South State Route 157  
20 Edwardsville, Illinois 62025  
21 Telephone: (618) 656-5150  
22 [tom@ghalaw.com](mailto:tom@ghalaw.com)  
23 [kevin@ghalaw.com](mailto:kevin@ghalaw.com)  
24 [thorscroft@ghalaw.com](mailto:thorscroft@ghalaw.com)

25 Attorneys for Plaintiff

26 **UNITED STATES DISTRICT COURT**  
27 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

28 NATALIE TURCK, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

META PLATFORMS, INC., a Delaware  
corporation,

Defendant.

Case No:

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

**TABLE OF CONTENTS**

NATURE OF THE ACTION.....	1
PARTIES.....	6
JURISDICTION AND VENUE.....	6
COMMON FACTUAL ALLEGATIONS .....	7
I.    Illinois’ Protection of Biometric Data .....	7
II.   Meta Repeatedly Chooses Self-Interest Over User Privacy Interests .....	10
III.  Beginning in 2016, Meta Seeks and Obtains Patent Protections for its System of Identifying Facebook Users with Voiceprints, with Updates in 2020, 2022, and 2023 .....	12
IV.   Meta Possesses, Creates, Collects, Captures, Receives Through Trade, and/or Otherwise Obtains Biometric Identifiers and Biometric Information.....	22
V.    Meta’s Inadequate Disclosures Regarding Voiceprints .....	26
A.    Meta’s Privacy Center .....	26
B.    Facebook’s “Access Your Information” .....	33
C.    Meta’s Privacy Policy .....	37
D.    Meta’s United States Regional Privacy Notice .....	44
VI.   Plaintiff’s Experience .....	50
CLASS ACTION ALLEGATIONS.....	51
CLAIMS FOR RELIEF .....	54
COUNT I.....	54
COUNT II .....	56
COUNT III .....	57
COUNT IV .....	59
PRAYER FOR RELIEF .....	60
JURY DEMAND .....	61

1 **NOTICE TO DEFENDANT OF DUTIES TO RETAIN EVIDENCE:**

2 **TO DEFENDANT:** Note and adhere to your duties to retain, and not delete or destroy,  
3 all documents, emails, databases, electronic records, electronically stored information, and all  
4 other evidence that may be pertinent to this lawsuit, and to cease any destruction or deletion of  
5 such evidence that might otherwise take place in the ordinary course of your business or affairs.  
6

7  
8 Plaintiff, Natalie Turck, on behalf of herself and all others similarly situated, for her Class  
9 Action Complaint against Defendant Meta Platforms, Inc. (“Meta”), states as follows upon  
10 personal knowledge as to herself and her own acts and experiences, and, as to all other matters,  
11 upon information and belief, including investigation conducted by her attorneys.

12 **NATURE OF THE ACTION**

13 1. This claim involves Illinois’ Biometric Information Privacy Act, 740 ILCS 14/1  
14 *et seq.* (“BIPA”), a law that regulates companies that possess, collect, capture, obtain, store, and  
15 use Illinois citizens’ biometric data, such as voiceprints, fingerprints, and scans of face geometry,  
16 and information derived therefrom.  
17

18 2. Meta owns and operates the social media platform, Facebook.

19 3. Meta also owns and operates Messenger, a messaging app that can be used for,  
20 *inter alia*, instant messages, sharing photos, videos, recording and sending audio recordings,  
21 group chats, and video and audio calls.

22 4. This case involves Meta’s obtaining and possession of voiceprints and related  
23 biometric information from Illinois users of its Facebook and Messenger platforms in violation  
24 of BIPA.  
25

26 5. Under BIPA, Meta may not collect, capture, purchase, receive through trade, or  
27 otherwise obtain a person’s voiceprint unless it first obtained consent as set forth in BIPA §15(b),  
28

1 which provides that, before a voiceprint or related biometric information (collectively “biometric  
2 data”) is collected, captured, received through trade, or otherwise obtained, Meta is required to:  
3 (1) inform the person in writing that their biometric data is being collected or stored; (2) inform  
4 the person in writing of the specific purpose and length of term for which their biometric data is  
5 being collected, stored, and used; (3) receive a written release executed by the subject of the  
6 biometric data. 740 ILCS 14/15(b).

7  
8 6. At least in 2023, and upon information and belief, for many years prior, Meta has  
9 been capturing, creating, collecting, and storing voiceprints and other related biometric  
10 information of Facebook and Messenger users from audio submitted via Facebook or Messenger.

11 7. Meta’s maze of privacy policies nowhere accurately or fully describes its  
12 possession, capturing, collection, creating, obtaining, and use of voiceprints or other related  
13 biometric information. While Meta sought a patent in 2016 (issued in 2020) related to the use of  
14 voiceprints to identify users, which used the term “voiceprint” nearly 200 times, its disclosures  
15 to consumers nowhere uses the term.  
16

17 8. Nor does Meta purport to seek any affirmative consent from users in advance of  
18 such capture, collection, creation, storage, and/or obtaining of voiceprints or related biometric  
19 information.

20 9. In fact, it was not until January 2023 that Meta updated its Privacy Policy to  
21 vaguely acknowledge that “[t]he categories of Personal Information we may have collected about  
22 you over the past 12 months,” “may” have included “voice recordings” that “may be used to  
23 identify you.”  
24

25 10. That statement buried in Meta’s website does not come close to satisfying the  
26 requirements of BIPA § 15(b).  
27  
28

1           11.     Meta also lacks a retention and destruction policy for biometric data that complies  
2 with BIPA §15(a), which requires Meta to have a public written policy outlining that it will  
3 permanently destroy the biometric data once the initial purpose for its collection has been  
4 satisfied or within three years of the user’s last interaction with Meta, whichever is earlier. 740  
5 ILCS 14/15(a).

6           12.     Instead, Meta’s stated retention/destruction policy is to hold biometric data until  
7 it decides it no longer needs it: “We keep Personal Information, including sensitive Personal  
8 Information, as long as we need it to provide our products, comply with legal obligations or  
9 protect our or other’s interests. We decide how long we need information on a case-by-case  
10 basis.”

11           13.     As a result of this “we decide” policy, Meta has unlawfully retained the biometric  
12 data of Plaintiff and the Class in violation of BIPA §15(a).  
13

14           14.     Meta also violates BIPA §15(c), which prohibits entities in possession of  
15 biometric data from selling, leasing, trading, or otherwise profiting from a person’s biometric  
16 data. 740 ILCS 14/15(c). Meta profits off of the biometric data of Plaintiff and the Class in its  
17 possession by, *inter alia*, using the biometric data to improve its voice recognition and  
18 identification methods, software, processors, and machine learning; improve its products and  
19 product development for hardware and software that utilize voice recognition, such as user  
20 authentication features; and using biometric data to identify users so that it can send them  
21 customized, targeted content, including targeted advertisements.  
22

23           15.     At its core, Meta is a digital advertising company. As self-described in its most  
24 recent Annual Report filed with the United States Securities and Exchange Commission, “we  
25 generate substantially all of our revenue from selling advertising placements on our family of  
26  
27  
28

1 apps to marketers . . . . Marketers purchase ads that can appear in multiple places including on  
2 Facebook, Instagram, Messenger, and third-party applications and websites.”<sup>1</sup>

3 16. Meta also explained in its 2022 Annual Report that it was “making significant  
4 investments in artificial intelligence and machine learning to improve our delivery, targeting, and  
5 measurement capabilities” as a way of mitigating legislative and regulatory developments that  
6 have “impacted our ability to use data signals in our ad products.”<sup>2</sup>

7  
8 17. In 2022, Meta generated over \$113.6 billion in advertising revenue alone, which  
9 constituted over 97% of Meta’s total annual revenue.<sup>3</sup>

10 18. Ultimately, Meta profits from the biometric data of Plaintiff and the Class by,  
11 *inter alia*, using the biometric data to allow Meta to more effectively target users with ads and  
12 thus sell more of Meta’s main product (targeted advertisements) to Meta’s primary customers  
13 (advertisers).

14 19. Finally, Meta violates BIPA § 15(e), which requires entities in possession of  
15 biometric data to store, transmit, and protect from disclosure all biometric data using the  
16 reasonable standard of care in the industry and in a manner that is the same as or more protective  
17 than the manner in which the entity stores, transmits, and protects other confidential and sensitive  
18 information. 740 ILCS 14/15(e).

19  
20 20. Meta’s 2020 Annual Report explained that “[o]ur industry is prone to cyber-  
21 attacks by third parties seeking unauthorized access to our data or users’ data,” and further  
22 explained that “[a]s a result of our prominence, the size of our user base, the types and volume  
23 of personal data and content on our systems, and the evolving nature of our products and services  
24

---

25  
26 <sup>1</sup> Meta 2022 10-K, p. 7,  
<https://www.sec.gov/Archives/edgar/data/1326801/000132680123000013/meta-20221231.htm>.

27 <sup>2</sup> *Id.* p. 56.

28 <sup>3</sup> *Id.* p. 99.

1 (including our efforts involving new and emerging technologies), we believe that we are a  
2 particularly attractive target for such breaches and attacks . . . .”<sup>4</sup>

3 21. In September 2018, Meta announced the discovery of a third-party cyber-attack  
4 “that exploited a vulnerability in Facebook’s code to steal user access tokens, which were then  
5 used to access certain profile information from approximately 29 million user accounts on  
6 Facebook.”<sup>5</sup>

7 22. In the 2022 Annual Report, Meta stated: “[W]e have discovered and announced,  
8 and anticipate that we will continue to discover and announce, additional incidents of misuse of  
9 user data or other undesirable activity by third parties.”

10 23. Meta further acknowledged that, because of factors such as its size and how it  
11 allocates its resources, it is simply unable to discover all intrusions into its user data by third  
12 parties: “We may not discover all such incidents or activity, whether as a result of our data or  
13 technical limitations, including our lack of visibility over our encrypted services, the scale of  
14 activity on our platform, the allocation of resources to other projects, or other factors, and we  
15 may be notified of such incidents or activity by the independent privacy assessor required under  
16 our modified consent order with the FTC, the media, or other third parties. Such incidents and  
17 activities have in the past, and may in the future, include the use of user data or our systems in a  
18 manner inconsistent with our terms, contracts or policies, the existence of false or undesirable  
19 user accounts, election interference, improper advertising practices, activities that threaten  
20 people’s safety on- or offline, or instances of spamming, scraping, data harvesting, unsecured  
21  
22  
23  
24  
25  
26

---

27 <sup>4</sup> *Id.* p. 42.

28 <sup>5</sup> *Id.* p. 43.

1 datasets, or spreading misinformation. We may also be unsuccessful in our efforts to enforce our  
2 policies or otherwise remediate any such incidents.”<sup>6</sup>

3 24. Accordingly, Plaintiff seeks to represent a class of similarly situated individuals  
4 to obtain an Order: (A) awarding Plaintiff and each Class Member statutory damages of \$5,000  
5 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, in the  
6 alternative, statutory damages of \$1,000 for each negligent violation of BIPA pursuant to 740  
7 ILCS 14.20(1); (B) enjoining Meta from possessing, collecting, obtaining, storing, using, selling,  
8 leasing, trading, and profiting from Plaintiff’s and the Class Members’ biometric data until done  
9 so in compliance with BIPA; (C) awarding Plaintiff and the Class Members reasonable attorneys’  
10 fees, costs, and other expenses pursuant to 740 ILCS 14/20(3); (D) awarding Plaintiff and the  
11 Class Members pre-and post-judgment interest, as provided by law; and (E) awarding such other  
12 and further relief as is just and appropriate.  
13

#### 14 **PARTIES**

15 25. Plaintiff is a natural person and citizen of the State of Illinois.

16 26. Meta is a Delaware corporation with its principal place of business in California.  
17  
18 It is, therefore, a citizen of Delaware and California.

#### 19 **JURISDICTION AND VENUE**

20 27. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C.  
21 § 1332(d). Because Plaintiff, who is a member of the Class, and Defendant are citizens of  
22 different States, there is minimal diversity. The total claims of Class Members exceed \$5,000,000  
23 exclusive of interest and costs. There are at least 100 Class Members.  
24

25 28. This Court has personal jurisdiction over Defendant because it has its principal  
26 places of business in California and is, therefore, a citizen of California.  
27

---

28 <sup>6</sup> *Id.*



29. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendant resides in this district and is a resident of the State in which this district is located.

### **COMMON FACTUAL ALLEGATIONS**

#### **I. Illinois' Protection of Biometric Data**

30. The Illinois General Assembly enacted the Biometric Information Privacy Act, 740 ILCS 14/*et seq.* ("BIPA") in 2008 to establish standards of conduct for private entities that collect or possess biometric identifiers and biometric information.

31. "Biometric identifiers" covered by BIPA include retina or iris scans, fingerprints, voiceprints, and scans of human or face geometry. 740 ILCS 14/10.

32. "Biometric information" covered by BIPA includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

33. The Illinois General Assembly noted that BIPA was carefully crafted to protect biometric data because "unlike other unique identifiers that are used to access finances or other sensitive information," one's own biometric data cannot be changed; "[t]herefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5.

34. The legislative findings also acknowledge that "[t]he full ramifications of biometric technology are not fully known." *Id.* § 14/5(f). Accordingly, the General Assembly found that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *Id.* § 14/5(g).

35. The Seventh Circuit has also stated that biometric data is "meaningfully different" from other personal information, such as addresses, dates of birth, telephone numbers, and credit

1 card and social security numbers, because of the “inherent sensitivity of biometric data,” which  
2 is “immutable, and once compromised, [is] compromised forever—as the legislative findings in  
3 BIPA reflect.” *Fox v. Dakota Integrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020).

4 36. BIPA makes it unlawful for any private entity to, *inter alia*, “collect, capture,  
5 purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric  
6 identifier or biometric information unless it first: (1) informs the subject . . . in writing that a  
7 biometric identifier or biometric information is being collected or stored; (2) informs the subject  
8 . . . in writing of the specific purpose and length of term for which a biometric identifier or  
9 biometric information is being collected, stored, and used; and (3) receives a written release  
10 executed by the subject of the biometric identifier or biometric information . . . .” 740 ILCS  
11 14/15(b).  
12

13 37. Furthermore, BIPA requires that any “private entity in possession of biometric  
14 identifiers or biometric information must develop a written policy, made available to the public,  
15 establishing a retention schedule and guidelines for permanently destroying biometric identifiers  
16 and biometric information when the initial purpose for collecting or obtaining such identifiers or  
17 information has been satisfied or within 3 years of the individual’s last interaction with the  
18 private entity, whichever occurs first.” 740 ILCS 14/15(a).  
19

20 38. BIPA also provides that “[n]o private entity in possession of a biometric identifier  
21 or biometric information may sell, lease, trade, or otherwise profit from a person’s or a  
22 customer’s biometric identifier or biometric information.” 740 ILCS 14/15(c).  
23

24 39. Finally, BIPA provides that “[a] private entity in possession of a biometric  
25 identifier or biometric information shall: (1) store, transmit, and protect from disclosure all  
26 biometric identifiers and biometric information using the reasonable standard of care within the  
27 private entity’s industry; and (2) store, transmit, and protect from disclosure all biometric  
28

1 identifiers and biometric information in a manner that is the same as or more protective than the  
2 manner in which the private entity stores, transmits, and protects other confidential and sensitive  
3 information.” 740 ILCS 14/15(e).

4 40. BIPA provides for a private right of action: “Any person aggrieved by a violation  
5 of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal  
6 district court against an offending party.” 740 ILCS 14/20.

7 41. The Illinois Supreme Court has explained that a person whose biometric  
8 identifiers are the subject of violations of section 15 of BIPA is “aggrieved” by the entity’s failure  
9 to comply with BIPA and is “entitled to seek recovery” under Section 14/20. *Rosenbach v. Six*  
10 *Flags Entm’t Corp*, 2019 IL 123186, ¶ 33 (“[W]hen a private entity fails to comply with one of  
11 section 15’s requirements, that violation constitutes an invasion, impairment, or denial of the  
12 statutory rights of any person or customer whose biometric identifier or biometric information is  
13 subject to the breach. Consistent with the authority cited above, such a person or customer would  
14 clearly be ‘aggrieved’ within the meaning of section 20 of the Act (*id.* § 20) and entitled to seek  
15 recovery under that provision. No additional consequences need be pleaded or proved. The  
16 violation, in itself, is sufficient to support the individual’s or customer’s statutory cause of  
17 action.”).

18 42. Under BIPA, “[a] prevailing party may recover ***for each violation***: (1) against a  
19 private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or  
20 actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly  
21 violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is  
22 greater; (3) reasonable attorneys’ fees and costs, including expert witness fees and other litigation  
23 expenses; and (4) other relief, including an injunction, as the State or federal court may deem  
24 appropriate.” *Id.* (emphasis added).  
25  
26  
27  
28

## II. Meta Repeatedly Chooses Self-Interest Over User Privacy Interests

43. Meta has a troubled history involving user privacy and the misuse of users' personal information, including biometric data.

44. Meta's practice seems to be to do whatever it needs to do to improve its products and bottom line, even if that conduct is at the expense of its users' privacy, and deal with privacy invasions after the fact.

45. In 2012, the Federal Trade Commission approved a Consent Order entered with Meta to resolve charges brought by the FTC that Facebook deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. *See In re: Facebook, Inc.*, File No. 0923184 (FTC). The 2012 FTC Order required Meta to, *inter alia*, "not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to . . . its collection or disclosure of any covered information." *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135, \*6 (F.T.C. July 27, 2012). "Covered information" meant "information from or about an individual consumer." *Id.* at \*4.

46. In 2019, the United States filed a Complaint for Civil Penalties, Injunction, and Other Relief for Meta's violations of the 2012 FTC Order, seeking "to hold Facebook accountable for its failure to protect consumers' privacy as required by the 2012 Order and the FTC Act." *See United States v. Facebook, Inc.*, No. 1:19-cv-02184, ECF Dkt. 1, p. 1 (July 24, 2019).

47. The same day, Meta entered a Stipulated Order, in which it, *inter alia*, agreed to pay a civil penalty of \$5,000,000,000. *Id.* ECF Dkt. 2-1, ECF p. 3. Meta also agreed to modify the 2012 FTC Order in numerous ways, one of which included specifically listing "biometric information" as an example of "information from or about an individual consumer" in the

1 definition of “covered information.” *Id.* at ECF p. 11. The Modified Order also required Meta to  
 2 delete any existing Facial Recognition Templates, clearly and conspicuously disclose in a stand-  
 3 alone disclosure separate and apart from any privacy policy, data policy, or other similar page,  
 4 how Meta would use and share facial recognition templates, and obtain affirmative express  
 5 consent before creating any new facial recognition templates. *Id.* at ECF p. 16. Further, Meta  
 6 agreed to internal procedures, safeguards, and reporting obligations related to the introduction of  
 7 any “modified product, service, or practice that includes a material change in the collection, use,  
 8 or sharing of Covered Information; a product, service, or practice directed to minors; or a product,  
 9 service, or practice involving health, financial, biometric, or other similarly sensitive  
 10 information.” *Id.* at ECF pp. 17-19.<sup>7</sup>

12 48. On May 3, 2023, the FTC issued an Order to Show Cause alleging violations of  
 13 the Modified 2012 FTC Order and seeking further modifications. *In re Facebook, Inc.*, File No.  
 14 2123091 (F.T.C.).

16 49. In addition to charges from the FTC, Meta has previously faced, and settled, civil  
 17 litigation based on allegations that it allowed third parties, including Cambridge Analytica, to  
 18 access users’ personal information without consent. *See In re: Facebook, Inc. Consumer Privacy*  
 19 *User Profile Litig.*, No. 3:18-md-02843-VC (N.D. Cal.).

20 50. Meta is currently facing civil litigation alleging that it has collected the health  
 21 information of Facebook users from third parties without the users’ consent. *See, e.g., Doe v.*  
 22 *Meta Platforms, Inc.*, No. 5:22-cv-03580-NC (N.D. Cal.).

---

26 <sup>7</sup> The Stipulated Order was entered by the United States District Court for the District  
 27 of Columbia on April 23, 2020. *United States v. Facebook, Inc.*, 456 F. Supp. 3d 115 (D.D.C.  
 28 2020). Thereafter, the FTC entered its Order modifying the 2012 Order. *In re Facebook, Inc.*,  
 2020 FTC LEXIS 80, \*4 (F.T.C. April 27, 2020).

51. Meta has previously settled, and faces continuing litigation, based on its obtaining scans of face geometry without consent in violation of BIPA and other similar state laws. *See In re: Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747-JD (N.D. Cal.); *Texas v. Meta Platforms, Inc.*, No. 22-0121 (Tex. Ct. [71st Dist.] 2022).

### **III. Beginning in 2016, Meta Seeks and Obtains Patent Protections for its System of Identifying Facebook Users with Voiceprints, with Updates in 2020, 2022, and 2023**

52. In December 2016, Meta (then Facebook, Inc.) filed a patent application titled: “User Identification with Voiceprints on Online Social Networks.”

53. Meta sought to protect methods, software, and processors for identifying users of its social network with voiceprints created from audio input into the social network site or related applications (e.g., an audio message sent by a Facebook user to another person via Messenger).

54. The patent was issued on March 31, 2020, Patent No. 10,607,148 (the “2020 Voiceprint Patent”).

55. The 2020 Voiceprint Patent explained some of Meta’s purposes for obtaining voiceprints, including, *inter alia*, (1) to identify users; (2) to associate voiceprints with unknown users; (3) to authenticate users; (4) and to identify users and provide the identified users with customized content.<sup>8</sup>

56. The 2020 Voiceprint Patent explained numerous uses for the methods, software, and processors protected by the patent, including how Meta can create voiceprints, use them to identify users, and store voiceprints:

A social-networking system may record and analyze a user’s voice to determine a digital voiceprint for the user. . . . The voiceprint may be received by a client system [e.g. a mobile device], stored on the social-networking system, and used to determine whether subsequently-received audio input is spoken by the same user. The social-networking system may use the voiceprint to identify or

---

<sup>8</sup> 2020 Voiceprint Patent, p. 4.

1 authenticate a user based on audio input, and then perform actions  
2 based on voice commands in the audio input. . . . A voiceprint may  
3 be generated based on the audio input and stored in the data store  
4 as the user's voiceprint.<sup>9</sup>

5 57. In addition, the 2020 Voiceprint Patent explained that Meta can create and store  
6 voiceprints of its users when audio of them is received, not from the user, but from other sources  
7 (e.g., other users), and that Meta can utilize its vast data sources to link the voiceprint with a user:

8 [T]he social-networking system may receive an audio input from  
9 an unknown user who is not associated with a voiceprint, and  
10 associate the audio input with a particular social-networking user  
11 and a probability that the audio input was spoken by the candidate  
12 user. A voiceprint may then be generated for the unknown user  
13 based on the audio input and associated with the candidate user and  
14 the probability. The candidate user and the probability may be  
15 identified by correlating where or when the audio input was  
16 received with the candidate user's social-networking information  
17 and information about any known users who may be connected to  
18 the candidate user in the social-networking system and/or located  
19 at or near the location of the candidate user.<sup>10</sup>

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

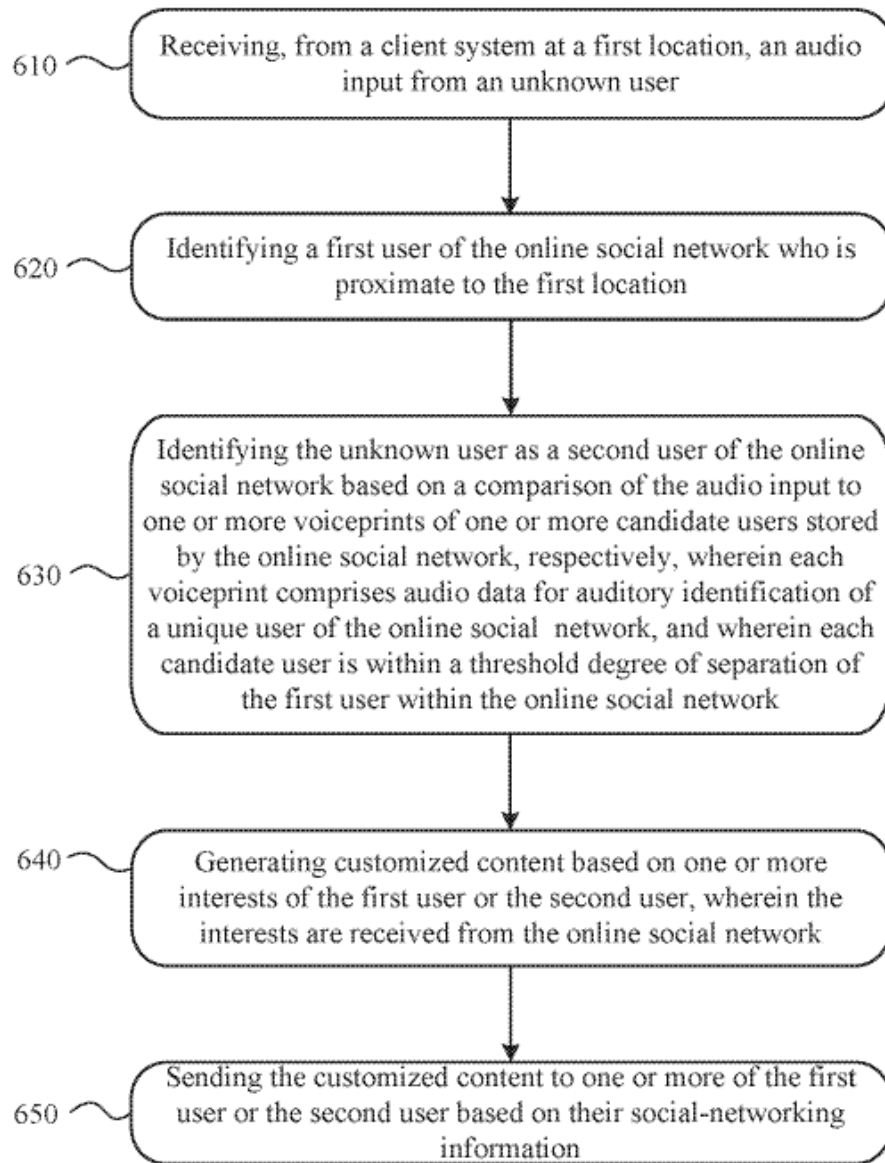
28 ///

---

<sup>9</sup> *Id.* at 2.

<sup>10</sup> *Id.* at 3.

58. The 2020 Voiceprint Patent illustrates an example of providing customized content after voiceprint identification of an initially unknown user:<sup>11</sup>



59. The 2020 Voiceprint Patent provided examples showing that “customized content” meant advertisements and other targeted content:

A client device associated with the social-networking system may detect one or more people speaking, and the people speaking may be identified as users based on comparison of their voices to voiceprints stored by the social-networking system. Upon identifying one or more of the people as users of the social-

<sup>11</sup> *Id.* at Fig. 6.



1           networking system, the social-networking system may provide  
2           customized content to the identified users based on their social-  
3           networking information. The customized content may be  
4           personalized to match the interests of the identified users, and may  
5           include advertisements, news feeds, push notifications, place tips,  
6           coupons, or suggestions.<sup>12</sup>

7           60.     The 2020 Voiceprint Patent also explained that Meta may receive audio input  
8           from an unknown user, which it can compare to voiceprints of Facebook users to identify and  
9           target with customized content:

10           [T]he social-networking system may receive, from a client  
11           system at a first location, an audio input from an unknown  
12           user. . . . [T]he social-networking system may identify a first  
13           user of the online social network who is proximate to the first  
14           location. As an example and not by way of limitation, the online  
15           social network may receive the identity of a user proximate to the  
16           first location by searching the known locations of users for  
17           locations that are within a threshold distance of the first location.  
18           The known locations of a user may be determined by the online  
19           social network based on the user's use of a client system that has  
20           sent its geographical location to the online social network, based on  
21           the user checking-in at the geographical location, based on  
22           identifying the user's voice at the geographical location via  
23           voiceprint analysis, or based on other techniques described  
24           herein. . . .

25           [T]he social-networking system may identify the unknown user as  
26           a second user of the online social network based on a comparison  
27           of the audio input to one or more voiceprints of one or more  
28           candidate users stored by the online social network, respectively,  
29           wherein each voiceprint comprises audio data for auditory  
30           identification of a unique user of the online social network, and  
31           wherein each candidate user is within a threshold degree of  
32           separation of the first user within the online social network. . . .

33           [T]he social-networking system may send customized content to  
34           one or more of the first user or the second user based on their social-  
35           networking information. . . . [T]he customized content may  
36           comprise content associated with the first location. . . . [T]he social-  
37           networking system may generate the customized content based on  
38           one or more interests of the first user or the second user, wherein  
39           the one or more interests are received from the online social  
40           network. . . . [T]he customized content may comprise content

---

<sup>12</sup> *Id.* at 32 (diagram numbers omitted).

1           having one or more topics that match the interests of the first user or  
 2           the second user. . . . [T]he customized content may comprise  
 3           advertisements, news feeds, push notifications, place tips, coupons,  
 4           suggestions, or a combination thereof.<sup>13</sup>

5           61.     The 2020 Voiceprint Patent provided examples of how audio of multiple people  
 6           can be captured from a device that is connected to a known (authenticated) Facebook user, which  
 7           Meta can compare to stored voiceprints to identify the second person and push customized  
 8           content to both:

9                     [W]hen multiple speakers are detected in audio input received by a  
 10                    client device of the social-networking system, the social-  
 11                    networking system may use voiceprint analysis to identify social  
 12                    network users who are connected to a known seed user, such as an  
 13                    authenticated user, e.g., the owner of a listening phone, and then  
 14                    send content to one or more of the social network users based on  
 15                    their interests. For example, suppose that two users, Marsha and  
 16                    Jan, are friends and are watching TV at Marsha's house. Marsha is  
 17                    an authenticated user of the TV at her house. A media  
 18                    device associated with the social-networking system (e.g., a dongle  
 19                    in communication with the TV) receives Jan's voice, and the social-  
 20                    networking system identifies Jan based on her voiceprint and on her  
 21                    social-graph connection to Marsha. Content or advertisements may  
 22                    then be provided to the users (e.g., to the TV, to Jan or Marsha's  
 23                    phone, etc.), and the content or advertisements may be customized  
 24                    to the interests of Marsha and Jan (e.g., the TV recommends a show  
 25                    or displays an advertisement for a product that both users are  
 26                    interested in). Content or advertisements may be provided to a  
 27                    group of three or more users if at least one of the users is an  
 28                    authenticated user.<sup>14</sup>

29           62.     The 2020 Voiceprint Patent also provided examples of how audio of multiple  
 30           people can be captured from a device that is not connected to a known (authenticated) Facebook  
 31           user, which Meta can still acquire, then compared to stored voiceprints to identify the people so  
 32           that Meta can push customized content to both people:

33                     [T]he social-networking system may use a process similar to that  
 34                    described above when the client device that detects speaking users  
 35                    is not authenticated to any of the speakers (for example, a

36                    

---

 37                    <sup>13</sup> *Id.* at 33-34 (diagram numbers omitted).

38                    <sup>14</sup> *Id.* at 32 (diagram numbers omitted).

1 BLUEETOOTH beacon in a public place). As an example, suppose  
 2 that Velma and Daphne walk into a store. Velma is known to be at  
 3 the store (e.g., she opens a mobile application from the store on her  
 4 smartphone). A beacon at the store may then detect Daphne  
 5 speaking, and the social-networking system may identify Daphne  
 6 based on a voiceprint analysis of Daphne's voice and based on  
 7 Velma and Daphne being socially connected. This identification  
 8 may occur even if the social-networking system does not otherwise  
 9 detect Daphne's presence in the store (e.g., because location  
 10 services, GPS, or the like are disabled or nonfunctional on her  
 11 phone). The social-networking system may then send content or  
 12 advertisements (e.g., a 2-for-1 coupon to the store; or an ad for a  
 13 nearby store that may have relevance to both users) to Velma's  
 14 and/or Daphne's device. Thus, in Daphne's case, content  
 15 customized for Daphne's location may be sent to her despite her  
 16 location services or GPS being disabled or non-functional.<sup>15</sup>

17 63. The 2020 Voiceprint Patent provided an example of another scenario by which  
 18 Meta can more easily identify users with their voiceprints by limiting the pool of users for the  
 19 voiceprint comparison based on an event:

20 [I]dentification of users may also be applied to an event, in which  
 21 case the event may correspond to a seed concept. For example,  
 22 suppose that a restaurant invites people to an event, and 100 users  
 23 confirm their attendance through the social-networking system.  
 24 The restaurant has a BLUEETOOTH beacon, and users may be  
 25 identified by comparing their captured voices to stored voiceprints  
 26 for the 100 attendees (as well as friends of the 100 attendees). In  
 27 this way, the social-networking system need not compare captured  
 28 voices to the voiceprints of social-network users who are not  
 29 attendees at the event. Instead, the search space for the voiceprint  
 30 comparison may be reduced from a large number of users of the  
 31 social-networking system to the relatively small number of users  
 32 who are associated with the event, such as the users who have  
 33 confirmed their attendance on the social-networking system, and  
 34 optionally their friends. Once attendees are identified, the social-  
 35 networking system may present information to them that is tailored  
 36 to their interests.<sup>16</sup>

37 64. The 2020 Voiceprint Patent provided an example of how users can be identified  
 38 even when the audio is obtained by a device with no authenticated users connected to it:

39 <sup>15</sup> *Id.* at 32-33 (diagram numbers omitted).

40 <sup>16</sup> *Id.* at 33 (diagram numbers omitted).

While the processes described above may involve a seed user or a seed concept, it is possible that initially there are no authenticated users. For example, suppose a user walks into a store and the location services or GPS on the user's client device are not active (e.g., BLUETOOTH is turned off and the client device does not have a good GPS signal). The BLUETOOTH beacon in the store receives the user's voice and the social-networking system identifies the user based on a comparison to voiceprints in the system. The system may compare the user's voice with many voiceprints to find a match. Alternatively, the system may apply filtering criteria based on time or location, e.g., to only consider voiceprints of users who have a recent location within a particular distance of the BLUETOOTH beacon.<sup>17</sup>

65. Accordingly, the 2020 Voiceprint Patent protected, *inter alia*, a method of, and software and processors for, using audio input of an unknown Facebook user (received by a known Facebook user) to identify the unknown Facebook user by comparing the audio input to the user's stored voiceprint:

What is claimed is:

1. A method comprising, by one or more computing devices of an online social network:

receiving, from a client system of a first user of the online social network, a first audio input from an unknown user;

identifying one or more candidate users, wherein each candidate user is a user of the online social network within a threshold degree of separation of a known user;

determining, for each candidate user, a proximity of the candidate user to the known user;

calculating, for each candidate user, a probability score representing a probability that the unknown user is the candidate user, wherein the probability score is based on the proximity of the candidate user and a ***comparison of the first audio input to a voiceprint of the candidate user stored by the online social network, wherein each voiceprint comprises audio data for auditory identification of the candidate user;*** and

---

<sup>17</sup> *Id.* (diagram numbers omitted).

identifying one of the candidate users as being the unknown user based on the calculated probability scores of the candidate users.

\* \* \* \*

14. One or more computer-readable non-transitory storage media embodying software that is operable when executed to:

receive, from a client system of a first user of an online social network, a first audio input from an unknown user;

identify one or more candidate users, wherein each candidate user is a user of the online social network within a threshold degree of separation of the first a known user;

determine, for each candidate user, a proximity of the candidate user to the known user;

calculate, for each candidate user, a probability score representing a probability that the unknown user is the candidate user, wherein the probability score is based on the proximity of the candidate user and a comparison of the first audio input to a voiceprint of the candidate user stored by the online social network, wherein each voiceprint comprises audio data for auditory identification of the candidate user; and

identify one of the candidate users as being the unknown user based on the calculated probability scores of the candidate users.<sup>18</sup>

66. The 2020 Voiceprint Patent also protected a method of generating and storing a new voiceprint for the unknown user based on other identifying information received:

What is claimed is:

\* \* \* \*

11. The method of claim 1, further comprising:

receiving identifying information for the unknown user;

---

<sup>18</sup> *Id.* at 51-52 (emphasis added). *See also id.* at ¶ 17 (claiming processors to perform the functions described above, including the “comparison of the first audio input to a voiceprint of the candidate user stored by the online social network”).

generating a new voiceprint based on the first audio input;  
and

storing the new voiceprint in association with the identity  
information for subsequent access by the online social  
network.<sup>19</sup>

67. On January 10, 2020, Meta filed a patent application that incorporated, and was a  
continuation of the 2020 Voiceprint Patent.

68. The patent was issued on October 18, 2022, Patent No. 11,475,344 (the “2022  
Voiceprint Patent”).

69. The 2022 Voiceprint Patent was substantially similar to the 2020 Voiceprint  
Patent, but made additional claims related to Meta’s method, software, and processors to, *inter*  
*alia*, use a voiceprint to identify a second user and authenticate access to an account.<sup>20</sup>

70. On August 26, 2022, Meta filed a patent application that incorporated, and was a  
continuation of the 2020 Voiceprint Patent and the 2022 Voiceprint Patent.

71. The patent was issued on May 2, 2023 (the “May 2023 Voiceprint Patent”).

72. The May 2023 Voiceprint Patent was substantially similar to the 2020 Voiceprint  
Patent, but made additional claims related to Meta’s method, software, and processors for  
determining what type of customizable content to deliver to a device of a first user based on  
audio of a second user received on the device of the first user:

What is claimed is:

1. A method comprising:

receiving, from a client system of a first user, an audio input  
from a second user, wherein a first user profile  
corresponding to the first user comprises first interest  
information associated with the first user, wherein a second

<sup>19</sup> *Id.* at 52-53.

<sup>20</sup> 2022 Voiceprint Patent, pp. 51-52.

1 user profile corresponding to the second user comprises  
2 second interest information associated with the second user;

3 determining, based on a comparison of the audio input to a  
4 voiceprint of the second user, wherein the voiceprint  
5 comprises audio data for auditory identification of the  
6 second user, whether the audio input comprises a query  
7 related to the first interest information and the second  
8 interest information; and

9 sending, to the client system, customized content for  
10 presentation to the second user, wherein the content is  
11 customized using the first interest information and the  
12 second interest information.<sup>21</sup>

13 73. On July 13, 2023, Meta filed a patent application that incorporated, and was a  
14 continuation of the 2020 Voiceprint Patent, the 2022 Voiceprint Patent, and the May 2023  
15 Voiceprint Patent (the “July 2023 Voiceprint Patent Application”).

16 74. The July 2023 Voiceprint Patent Application was substantially similar to the prior  
17 Voiceprint Patents, but made additional claims related to Meta’s method, software, and  
18 processors for identifying a second user from audio received from a *location*, rather than from a  
19 known first user, and sending customized content using Facebook interest information associated  
20 with the first or second user:

21 What is claimed is:

22 1. A method comprising:

23 receiving, from a client system at a first location, an audio  
24 input from an unknown user;

25 identifying a first user who is proximate to the first location;

26 identifying the unknown user as a second user based on a  
27 comparison of the audio input to one or more voiceprints of  
28 one or more candidate users accessible by the client system,  
respectively, wherein each voiceprint comprises audio data

---

<sup>21</sup> May 2023 Voiceprint Patent, p. 51-52. *See also id.* at 52-54 (claiming software and processors to carry out this method).

for auditory identification of a unique user, and wherein each candidate user is a contact of the first user; and

sending customized content to one or more of the first user or the second user, wherein the content is customized using interest information associated with the first or second user.

\* \* \* \*

3. The method of claim 1, further comprising generating the customized content based on one or more interests of the first user or the second user, wherein the one or more interests are accessed from an online social network.

4. The method of claim 3, wherein the customized content comprises content having one or more topics that match the interests of the first user or the second user.

5. The method of claim 1, wherein the customized content comprises advertisements, news feeds, push notifications, place tips, coupons, suggestions, or a combination thereof.

6. The method of claim 1, wherein the client system is a mobile phone, a Bluetooth beacon, or a media device operable to receive audio input.<sup>22</sup>

#### **IV. Meta Possesses, Creates, Collects, Captures, Receives Through Trade, and/or Otherwise Obtains Biometric Identifiers and Biometric Information**

75. Numerous features of Meta allow it to collect audio of users' voices. For example, Meta's Messenger, which allows parties to send messages to one another, allows a user to utilize voice to text dictation, create and send voice messages, record/send videos with sound, and make voice and video calls. Facebook likewise allows users to, *inter alia*, search Facebook using a voice search and record and/or upload audio or videos with audio.

76. Meta receives the audio input from users when they utilize an audio function on Facebook or Messenger, including when they, *inter alia*, dictate a text message to send via

---

<sup>22</sup> July 2023 Voiceprint Patent Application, p. 27-28 *See also id.* at 28 (claiming software and processors to carry out the method of claim 1).

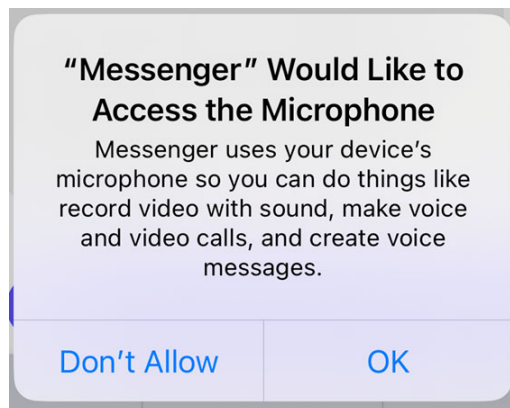


Messenger, send an audio recording via Messenger, make calls via Messenger, or provide audio data on Facebook, such as dictating a Facebook search, inputting their name pronunciation, posting an audio file, or posting a video that includes audio.

77. Upon information and belief, Meta also receives audio input of users from third party sources.

78. The audio input received by Meta can contain the voice of the person using the function or the voice of a person in the background.

79. Sometimes, a microphone is required to record audio or conduct a voice search. If the microphone function on a cell phone is turned off when a user seeks to utilize one of these audio functions on Messenger, Meta asks to “access the microphone,” with a pop up that states: “‘Messenger’ Would Like to Access the Microphone. Messenger uses your device’s microphone so you can do things like record video with sound, make voice and video calls, and create voice messages.”



80. The pop-up does not refer to any privacy policy, mention biometric data, or seek consent related to biometric data.

81. At least in 2023, and upon information and belief, for many years prior, Meta has been capturing, creating, collecting, and storing voiceprints and other biometric information of Facebook and Messenger users from audio data received via Facebook or Messenger and/or received from third parties.

1           82.     Upon information and belief, Meta not only captures, creates, collects, and stores  
2 voiceprints and related biometric information of users who themselves speak or upload audio via  
3 Facebook or Messenger; it also captures, creates, collects, and stores voiceprints and related  
4 biometric information of users whose voices are included in audio uploaded by others via  
5 Facebook or Messenger.

6           83.     From the audio input into Facebook or Messenger or otherwise received by Meta,  
7 Meta creates, captures, collects, stores, and/or obtains encoded digital data of the acoustic signals  
8 of the speaker's voice ("Digital Voice Data").  
9

10          84.     Meta processes the Digital Voice Data with, *inter alia*, an acoustical model, which  
11 is a model of the relationship between the audio signals and the sounds of phonetic units in the  
12 language.

13          85.     The acoustical model is trained, and further refined, using the voice of a particular  
14 user, such that the acoustical model can be used to recognize that user by voice.  
15

16          86.     The acoustical model is further trained using the voices of many users to produce  
17 a speaker-independent model capable of recognizing multiple users by their voice.

18          87.     Upon information and belief, Meta utilizes methods such as neural networks and  
19 deep learning models trained to extract distinctive characteristics of voices from the Digital  
20 Voice Data, such as the frequency pattern, frequency range, intonation, pitch, and accent, which  
21 output additional data based on the Digital Voice Data that can be and are used to identify an  
22 individual (the "Voice Characteristics").  
23

24          88.     Meta thus creates, captures, collects, stores, and/or obtains these Voice  
25 Characteristics.  
26  
27  
28

1           89.     Upon information and belief, Meta further creates and stores “Voice Profiles” for  
2 individual users, which store data specific to each individual user for use in subsequently  
3 recognizing each user by voice.

4           90.     The Digital Voice Data that Meta creates, captures, stores, and/or obtains is a  
5 dataset, unique to an individual, that, combined with other data and tools at Meta’s disposal, is  
6 capable of identifying that individual.

7           91.     Moreover, the Digital Voice Data that Meta creates, captures, collects, stores,  
8 and/or obtains is actually used by Meta to identify people.

9           92.     Meta’s most recent privacy policy acknowledges that the Digital Voice Data,  
10 which it calls voice recordings, can be used to identify a person. *See* Meta United States Regional  
11 Privacy Notice<sup>23</sup> (Meta may collect “voice recordings which may be used to identify you . . .”).

12           93.     Accordingly, the Digital Voice Data created, captured, collected, stored, and/or  
13 obtained by Meta constitutes a voiceprint, and thus, a “biometric identifier” under BIPA.

14           94.     Alternatively, the Voice Characteristics, and/or Voice Profiles constitute  
15 voiceprints, and thus, a “biometric identifier” under BIPA.

16           95.     Alternatively, the acoustical model, Voice Characteristics, and/or Voice Profiles  
17 are information based on a voiceprint used to identify an individual, and thus “biometric  
18 information” under BIPA.

19           96.     Upon information and belief, Meta creates, captures, collects, stores, and/or  
20 obtains other data that is based on a voiceprint and used to identify an individual, which  
21 additional data constitutes “biometric information” under BIPA.

22           97.     Upon information and belief, Meta uses the voiceprints and related biometric  
23 information in its possession to, *inter alia*, improve its voice recognition and identification  
24

25  
26  
27  
28           <sup>23</sup> <https://www.facebook.com/privacy/policies/uso/> (last visited Aug. 8, 2023).

1 methods, software, processors, and machine learning; to improve its products and product  
 2 development for hardware and software that utilize voice recognition, such as user authentication  
 3 features; and to identify users so that it can send them customized, targeted content, including  
 4 targeted advertisements.

## 5 **V. Meta's Inadequate Disclosures Regarding Voiceprints**

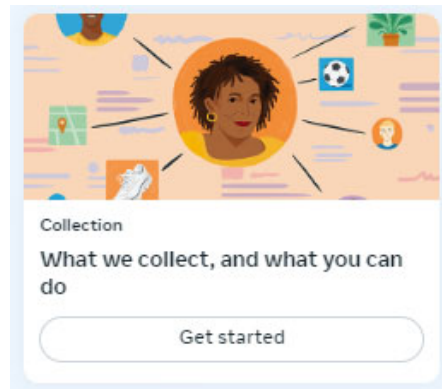
6 98. Meta's website purports to give users clear and easy access to information about  
 7 data it collects, but its statements regarding privacy are contained on multiple webpages, popups,  
 8 and supplemental terms, including in Meta's Privacy Center, an "Access Your Information"  
 9 section within one's Facebook account, a Privacy Policy, and a United States Regional Privacy  
 10 Policy.  
 11

12 99. Nowhere in these webpages, or anywhere else on its website, does Meta provide  
 13 the disclosures or policies required by BIPA.

### 14 **A. Meta's Privacy Center**

15 100. Meta's website contains a "Privacy Center" describing in general terms the  
 16 information it collects.  
 17

18 101. The Privacy Center contains a heading called "Collection," which states it covers  
 19 "What we collect, and what you can do."<sup>24</sup>



27  
28 <sup>24</sup> Meta Privacy Center Home, <https://www.facebook.com/privacy/center> (last visited Aug. 10, 2023).

1           102. Clicking “Get Started” leads to a new webpage that states: “Collecting your  
2 information helps us create better experiences on our products, so you can discover more of what  
3 you love. But we know many people want options to manage the information we’ve collected,  
4 so let’s talk about the control you have.”<sup>25</sup>

5           103. The webpage has links with menus that open popup windows for more  
6 information, shown in the screenshot below. One heading invites the user to “Learn about  
7 information we collect.” Another states: “Are Facebook and Instagram listening to your  
8 conversations?” The next states: “How can you delete your information.” There is also a button  
9 to “Review your information.” Other links reference the Privacy Policy, suggesting that is where  
10 users can find out “What information do we collect?” and “How you can manage or delete your  
11 information.” Other links state: “Learn how we use your information” and “You have options to  
12 manage the ads you see on Facebook.”  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

///

///

///

///

///

///

///

///


///

///

///

---

28           <sup>25</sup> <https://www.facebook.com/privacy/guide/collection> (last visited Aug. 10, 2023).



Collection

### What we collect, and what you can do

Collecting your information helps us create better experiences on our products, so you can discover more of what you love. But we know many people want options to manage the information we've collected, so let's talk about the control you have.

[Review your information](#)

- [Learn about information we collect](#)
- [Are Facebook and Instagram listening to your conversations?](#)
- [How can you delete your information?](#)

Learn more in the Privacy Policy

- [What information do we collect?  
Privacy Policy](#)
- [How can you manage or delete your information  
Privacy Policy](#)

More resources

- [Learn how we use your information  
Use](#)
- [You have options to manage the ads you see on Facebook  
Ads](#)

///

///

///

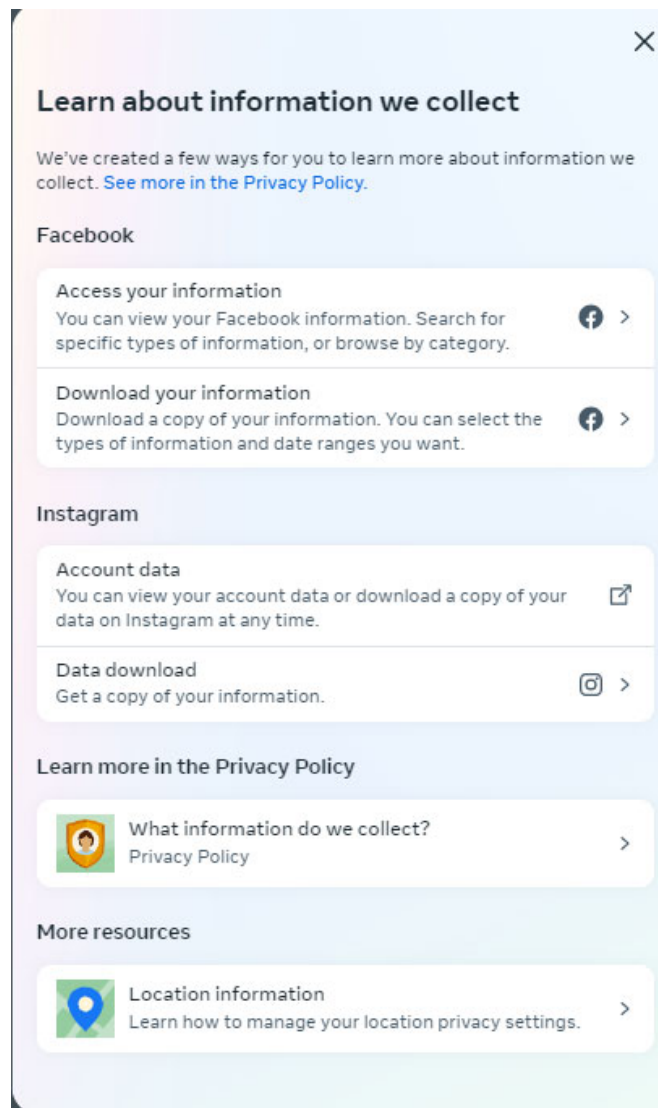
///

///

///

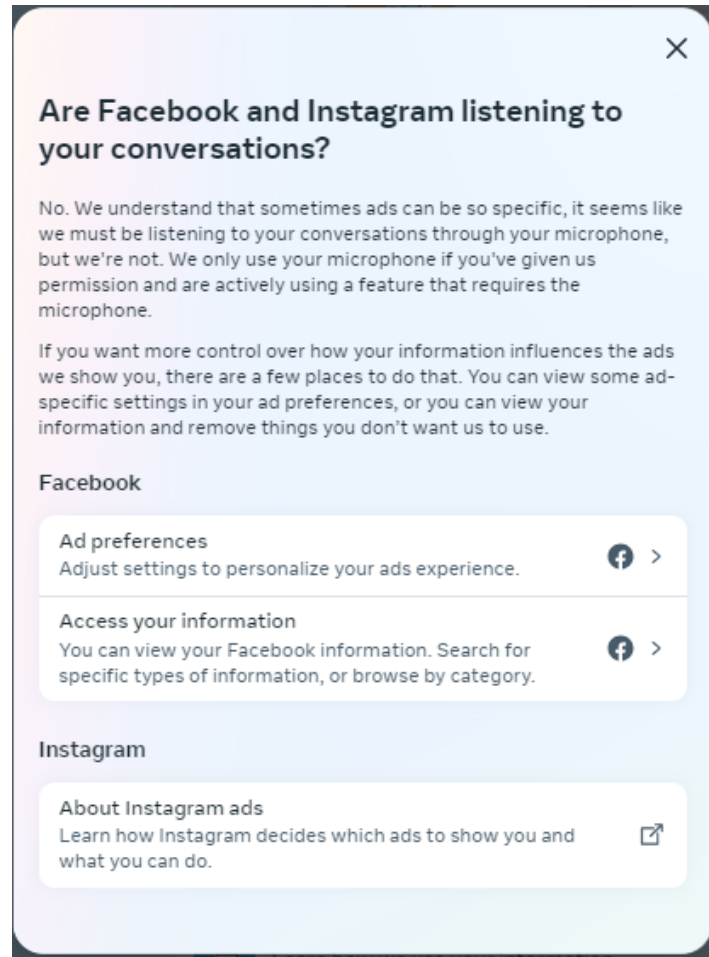
104. The link to “Review your information” leads to a Facebook login page. The user may log in to his or her Facebook account to obtain data Facebook provides about the user. As discussed in Section V.B below, nothing within those webpages discloses the existence of voiceprints or biometric information related thereto.

105. Clicking on “Learn about information we collect” opens a popup shown below<sup>26</sup> which provides another link to the Privacy Policy and links to access or download your information, both of which lead to the Facebook login page and process described above.



<sup>26</sup> Available at <https://www.facebook.com/privacy/dialog/what-we-collect> (last visited Aug. 10, 2023).

106. Returning to the “Collection” page and clicking “Are Facebook and Instagram listening to your conversations?” opens another popup shown below.<sup>27</sup> Meta states it is not listening to your conversations through your microphone, but states it uses your microphone with permission for certain audio features that require a microphone. There is no mention of what data is obtained when a user uses the microphone for one of those features.



///

///

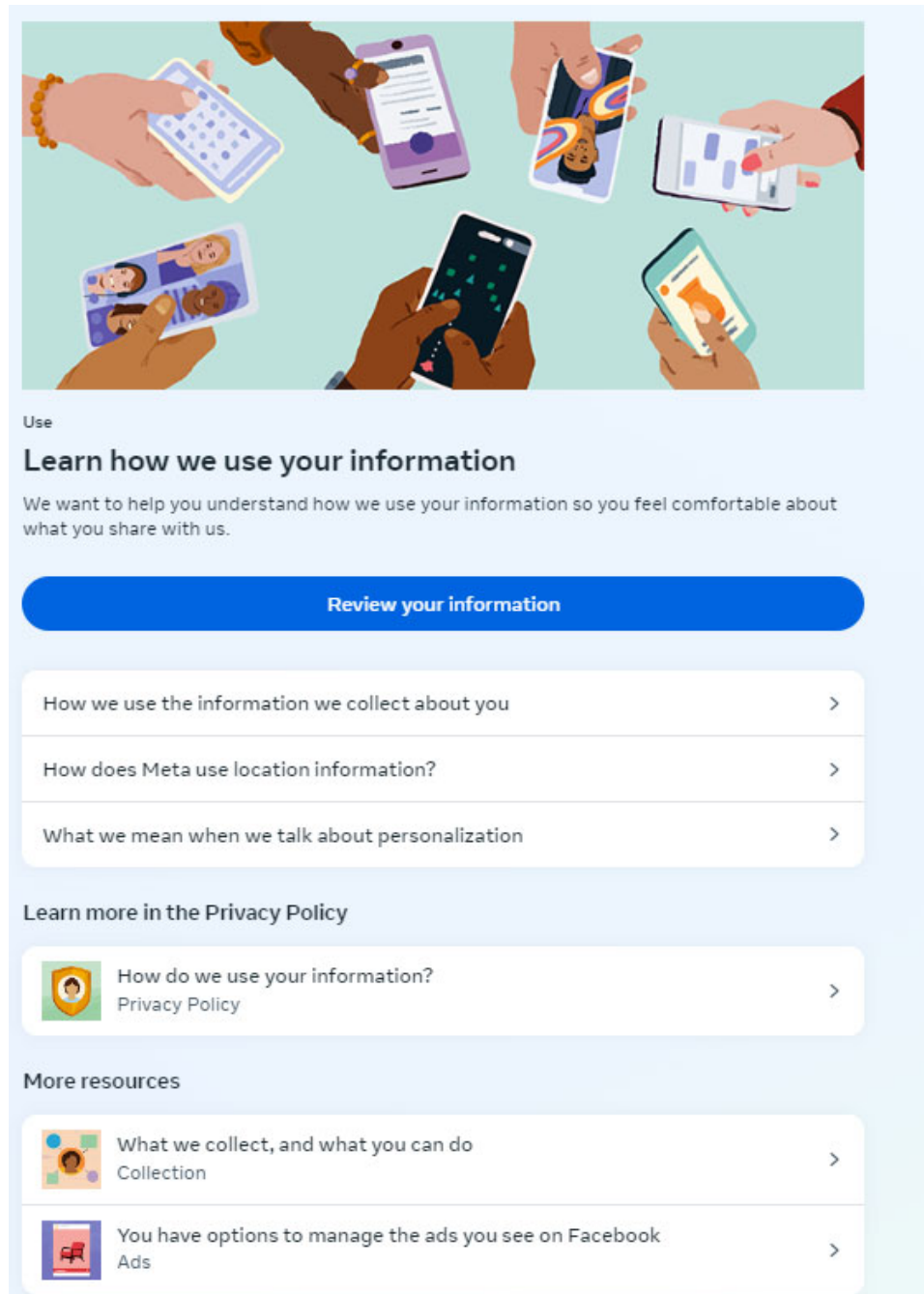
///

///

<sup>27</sup> Available at <https://www.facebook.com/privacy/dialog/is-facebook-listening-to-my-conversation> (last visited Aug. 10, 2023).

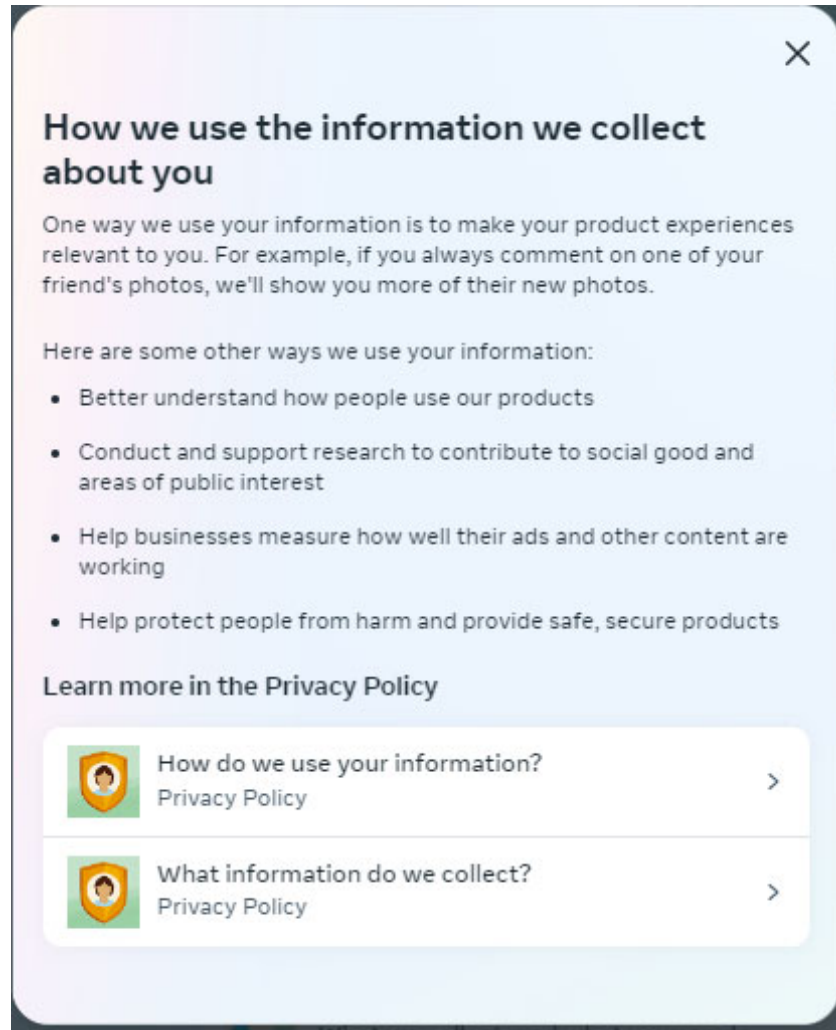


107. Returning to the “Collection” page and clicking “Learn how we use your information” opens another webpage shown below.<sup>28</sup>



<sup>28</sup> <https://www.facebook.com/privacy/guide/use/> (last visited Aug. 10, 2023).

108. Clicking on “How we use the information we collect about you” opens a popup shown below<sup>29</sup> that lists five ways Meta uses information it collects about users before directing them to the Privacy Policy:



///

///

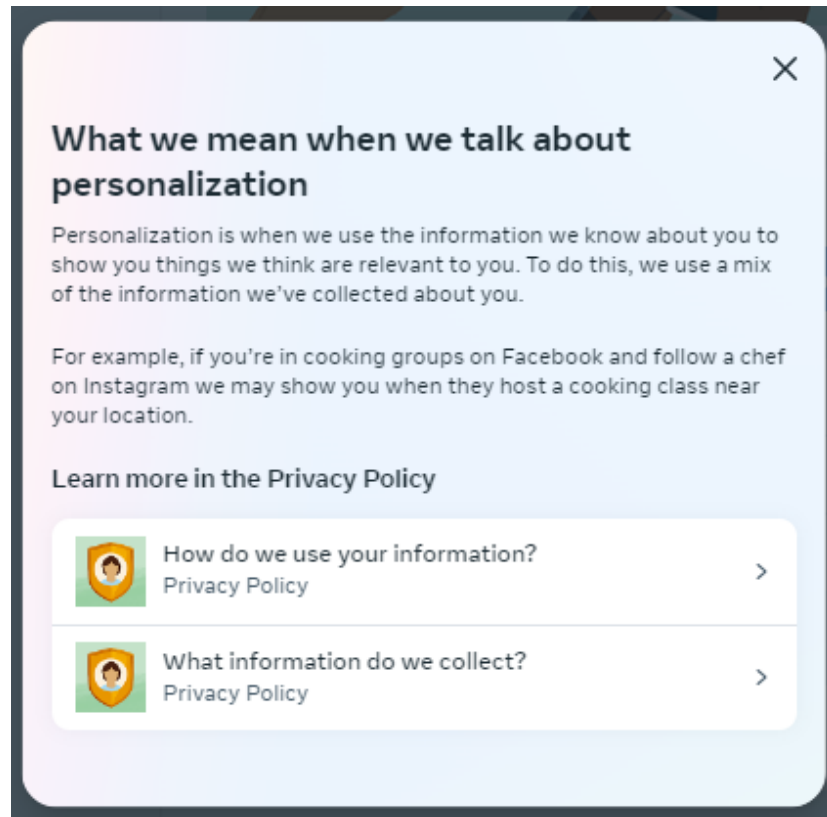
///

///

///

<sup>29</sup> Available at <https://www.facebook.com/privacy/dialog/how-we-use-collected-information> (last visited Aug. 10, 2023).

109. Returning to the “use” webpage and clicking “What we mean when we talk about personalization” opens a popup shown below<sup>30</sup> that directs users to the Privacy Policy and says, “[T]o show you things we think are relevant to you. . . . we use a mix of the information we’ve collected about you.”



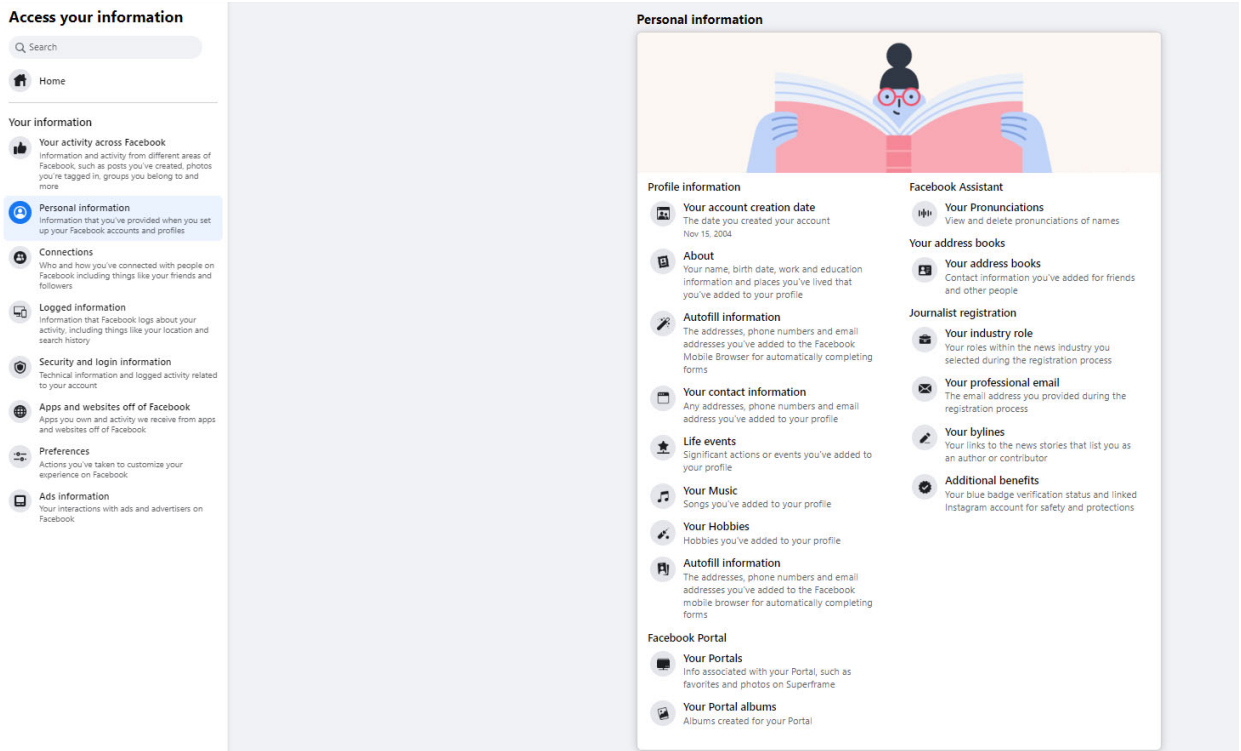
110. In short, nothing in this part of the Privacy Center discloses or describes the existence or use of voiceprints or biometric information related thereto.

#### **B. Facebook’s “Access Your Information”**

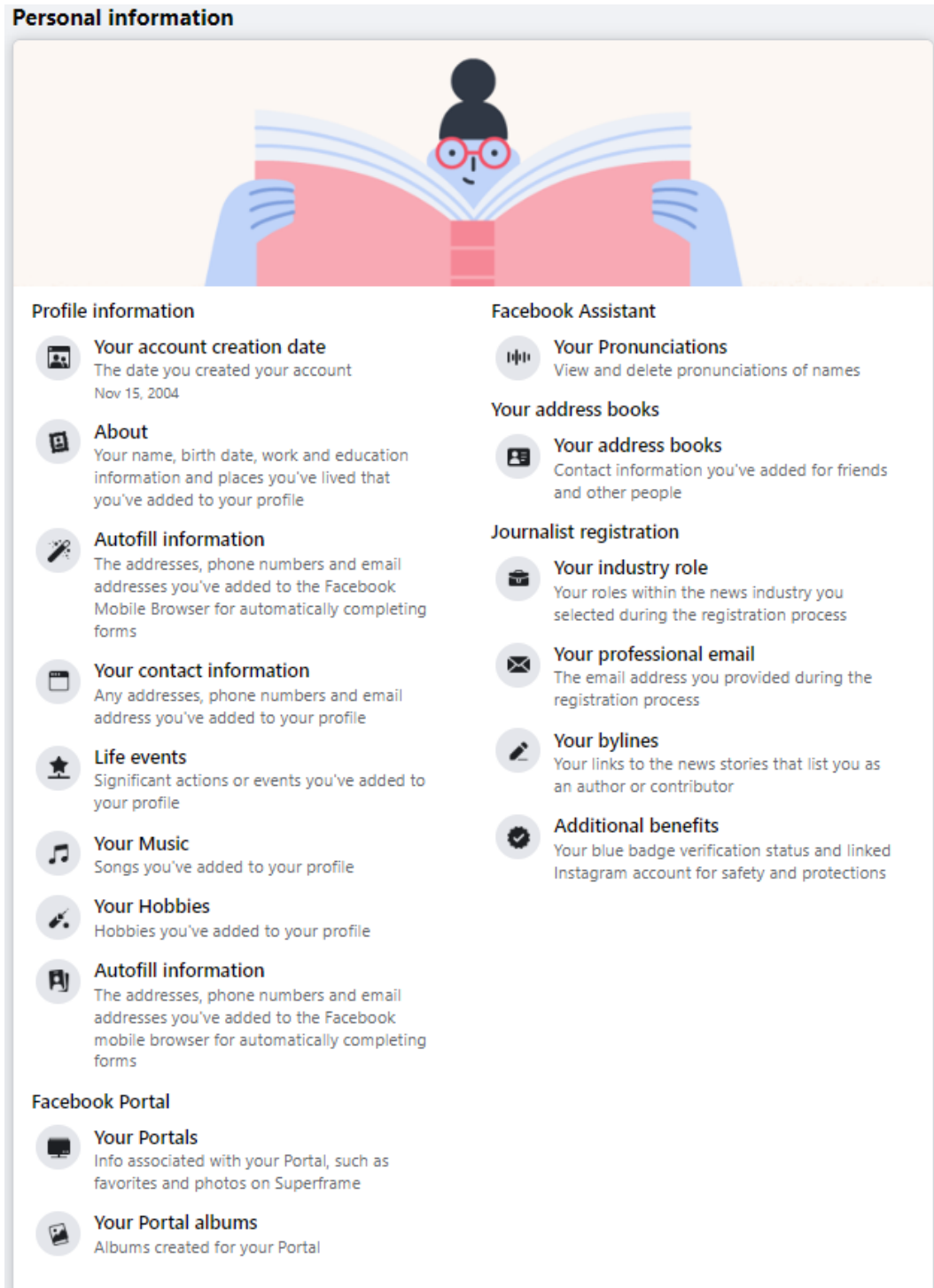
111. Likewise, nothing in the section of Facebook where a user can review or download his or her own information discloses the existence or use of voiceprints or biometric information related thereto.

<sup>30</sup> Available at <https://www.facebook.com/privacy/dialog/what-we-mean-when-we-talk-about-personalization> (last visited Aug. 10, 2023).

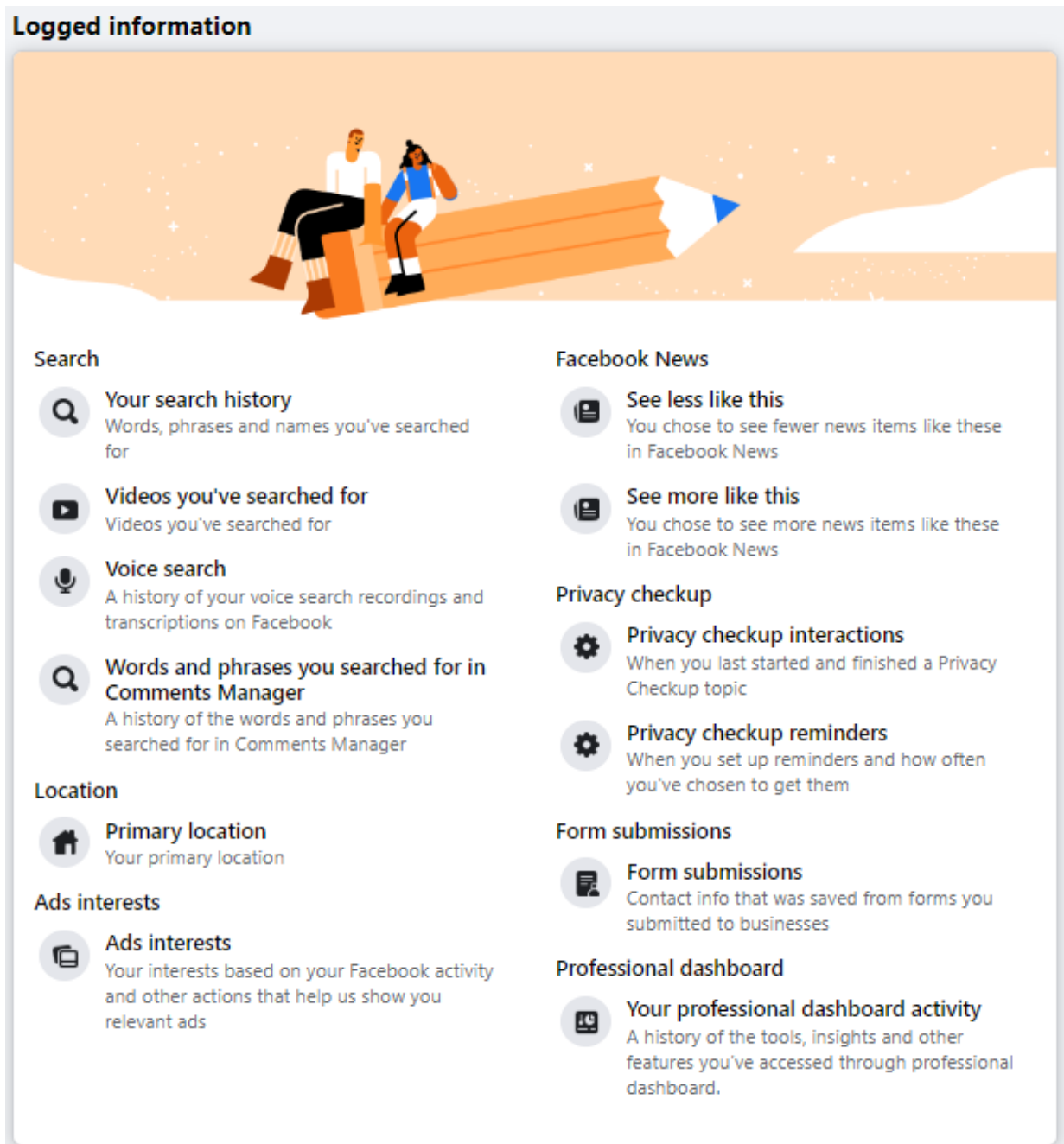
112. This section of Facebook shows the logged-in user what information Meta is willing to provide the user, as shown in the screenshot below:



113. Nothing in the “Personal Information” section indicates that Meta collects voiceprints or other related biometric information. Below is a zoomed-in screenshot of the image above:



114. As shown in the screenshot below, when a user seeks to access his or her “Logged information,” there is an indication that Meta has voice search recordings and transcriptions, but no indication that Meta collects voiceprints or other related biometric information.



115. No other section of the Access Your Information section of a user's Facebook profile mentions voiceprints or related biometric information.

### C. Meta's Privacy Policy

116. Likewise, nothing in Meta's Privacy Policy discloses the existence or use of voiceprints or biometric information related thereto.

117. The Privacy Policy states: "The information we collect and process about you depends on how you use our Products. For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our Products, we collect some information about you even if you don't have an account." It continues to describe "the information we collect" in categories of "Your activity and information you provide"; "Friends, followers and other connections"; "App, browser and device information"; and "Information from partners, vendors and other third parties."<sup>31</sup>

The information we collect and process about you depends on how you use our [Products](#). For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our Products, we collect some information about you [even if you don't have an account](#).

Here's the information we collect:

Your activity and information you provide >

Friends, followers and other connections >

App, browser and device information >

Information from partners, vendors and other third parties >

///

///

///

///

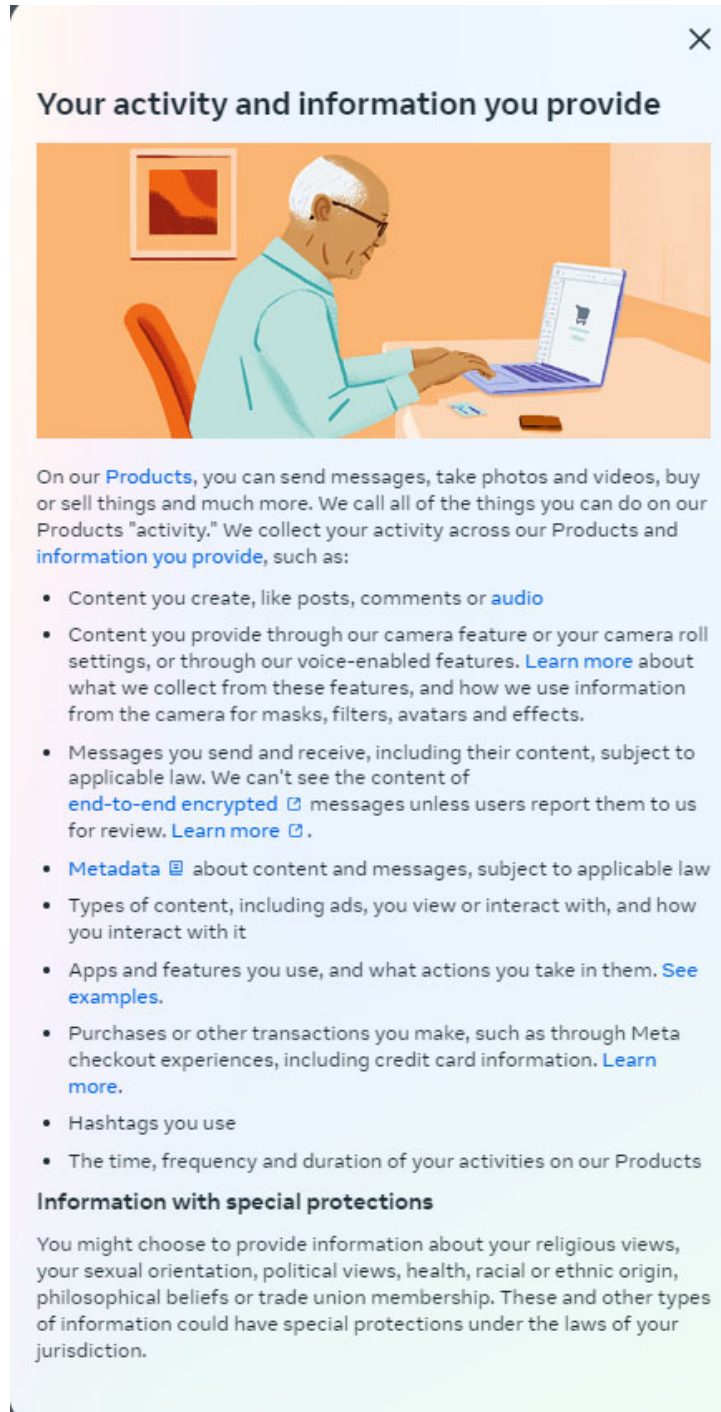
///

///

<sup>31</sup> Meta Privacy Policy, Effective June 15, 2023, <https://www.facebook.com/privacy/policy> (last visited Aug. 8, 2023).



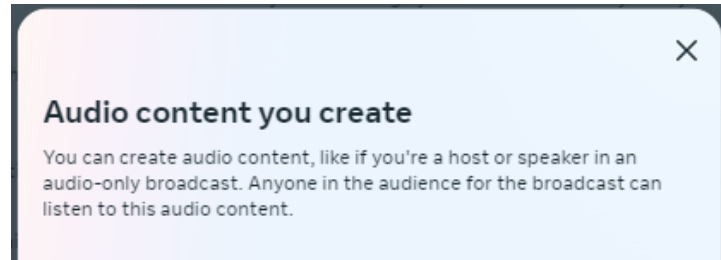
118. Clicking “Your activity and information you provide” opens a popup shown below,<sup>32</sup> which explains that “activity” means anything done on a Meta Product, and includes “[c]ontent you create, like posts, comments or audio.”



<sup>32</sup> Available at <https://www.facebook.com/privacy/policy?subpage=1.subpage.1-YourActivityAndInformation> (last visited Aug. 8, 2023).

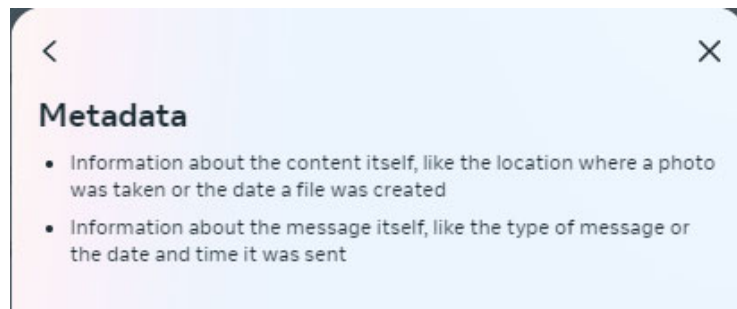


119. Clicking on the link “audio” opens another popup shown below<sup>33</sup> that simply states a user “can create audio content.”



120. Returning to the prior popup and clicking on the link to “Learn More” about “what we collect from” “our voice-enabled features” opens another popup<sup>34</sup> that provides an example of Meta collecting a voice interaction with Meta’s voice-enabled assistant on its Ray-Ban Stories product. There is no mention of voiceprints or related biometric data, or of such information obtained from Facebook or Messenger.

121. Returning to the prior popup and clicking on the link to “Metadata” opens a new popup shown below<sup>35</sup> that generally states metadata is information about the content or message:

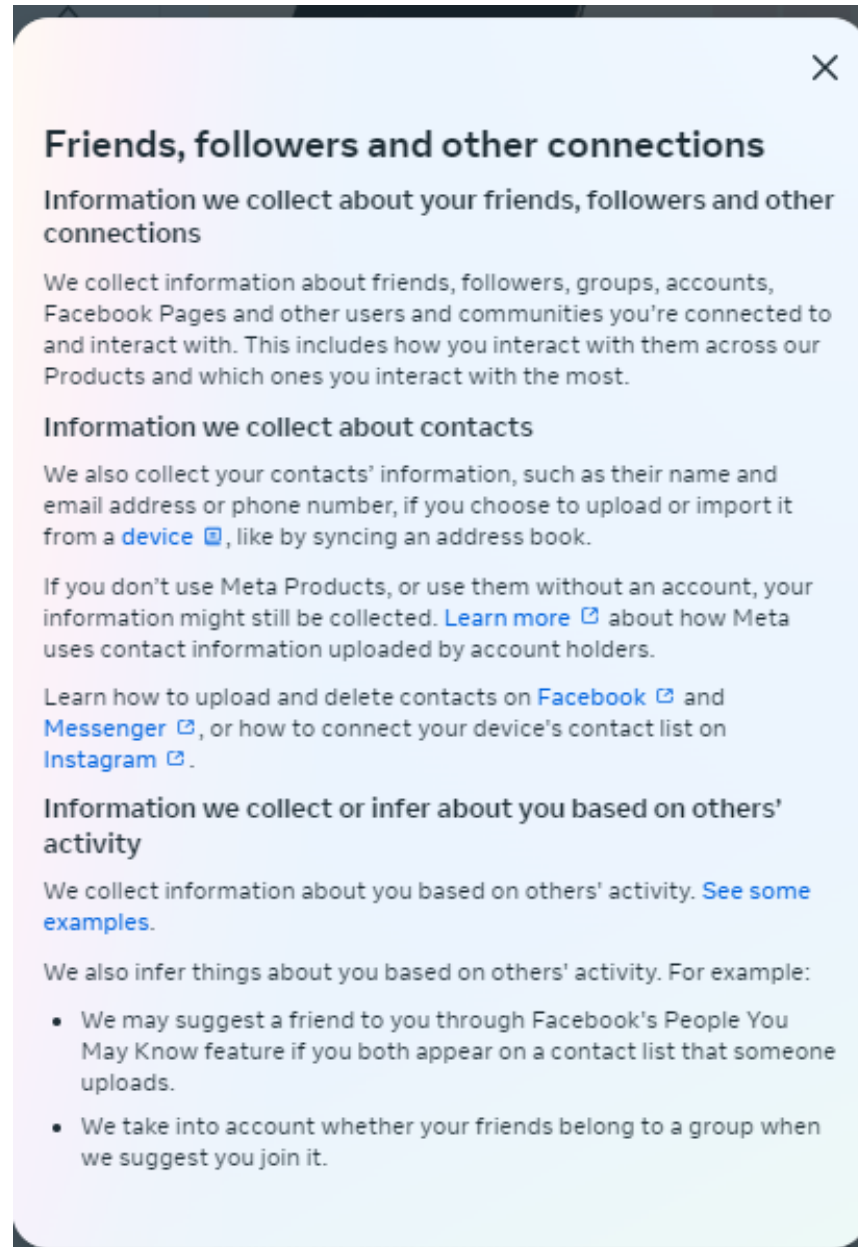


<sup>33</sup> Available at [https://www.facebook.com/privacy/policy?annotations\[0\]=1.ex.6-AudioContentYouCreate&subpage=1.subpage.1-YourActivityAndInformation](https://www.facebook.com/privacy/policy?annotations[0]=1.ex.6-AudioContentYouCreate&subpage=1.subpage.1-YourActivityAndInformation) (last visited Aug. 8, 2023).

<sup>34</sup> Available at [https://www.facebook.com/privacy/policy?annotations\[0\]=1.story.3-WhatWeCollectFrom&subpage=1.subpage.1-YourActivityAndInformation](https://www.facebook.com/privacy/policy?annotations[0]=1.story.3-WhatWeCollectFrom&subpage=1.subpage.1-YourActivityAndInformation) (last visited Aug. 8, 2023).

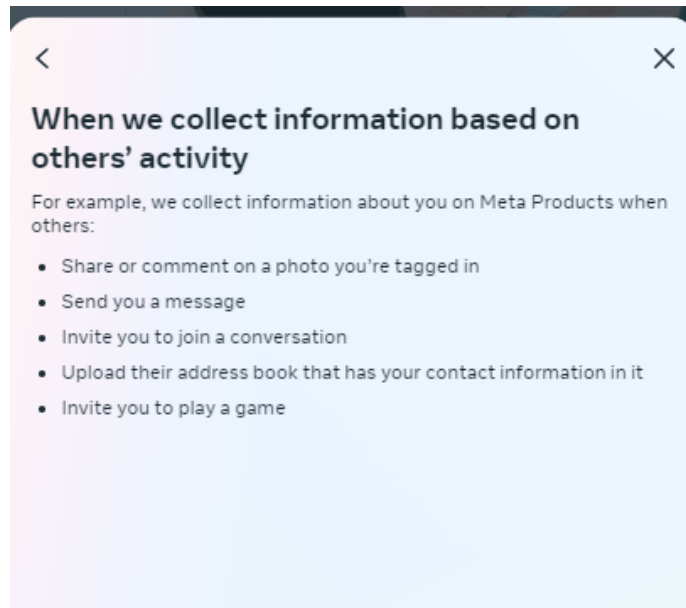
<sup>35</sup> Available at [https://www.facebook.com/privacy/policy?annotations\[0\]=Definition-Metadata&subpage=1.subpage.1-YourActivityAndInformation](https://www.facebook.com/privacy/policy?annotations[0]=Definition-Metadata&subpage=1.subpage.1-YourActivityAndInformation) (last visited Aug. 8, 2023).

122. Returning to the Privacy Policy and clicking the link discussing information collected from friends and followers vaguely indicates, “We collect information about you based on others’ activity,” as shown in the screenshot below:<sup>36</sup>




<sup>36</sup> Available at <https://www.facebook.com/privacy/policy?subpage=1.subpage.2-FriendsFollowersAndOther> (last visited Aug. 8, 2023).

123. Clicking on “See some examples” opens a popup shown below listing five examples, none of which indicate that audio of a user sent by another user may be used to create a voiceprint of the non-sending user or identify that user by comparing the audio to a voiceprint of the user.



124. Returning to the Privacy Policy and clicking the link discussing information collected from partners, vendors and other third parties opens a popup which states that Meta collects information from third parties “about a variety of your information and activities on and off our Products,” as shown in the screenshot below:<sup>37</sup>

<sup>37</sup> Available at <https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors> (last visited Aug. 8, 2023).





## Information from partners, vendors and other third parties


### What kinds of information do we collect or receive?

We collect and receive information from [partners](#), [measurement vendors](#), [marketing vendors](#) and [other third parties](#) about a variety of your information and activities on and off our [Products](#).

Here are some examples of information we receive about you:



- Your [device](#)  information
- Websites you visit and cookie data, like through Social Plugins or the Meta Pixel
- Apps you use
- Games you play
- Purchases and transactions you make off of our Products using non-Meta checkout experiences
- Your demographics, like your education level
- The ads you see and how you interact with them
- How you use our partners' products and services, online or in person

[Partners](#)  also share information like your email address, [cookies](#) and advertising device ID with us. This helps us match your activities with your account, if you have one.


We receive this information whether or not you're logged in or have an account on our Products. [Learn more](#)  about how we connect information from partners to your account.

Partners also share with us their communications with you if they instruct us to provide services to their business, like helping them manage their communications. To learn how a business processes or shares your information, read their privacy policy or contact them directly.

### Take control

 Off-Facebook activity
  >

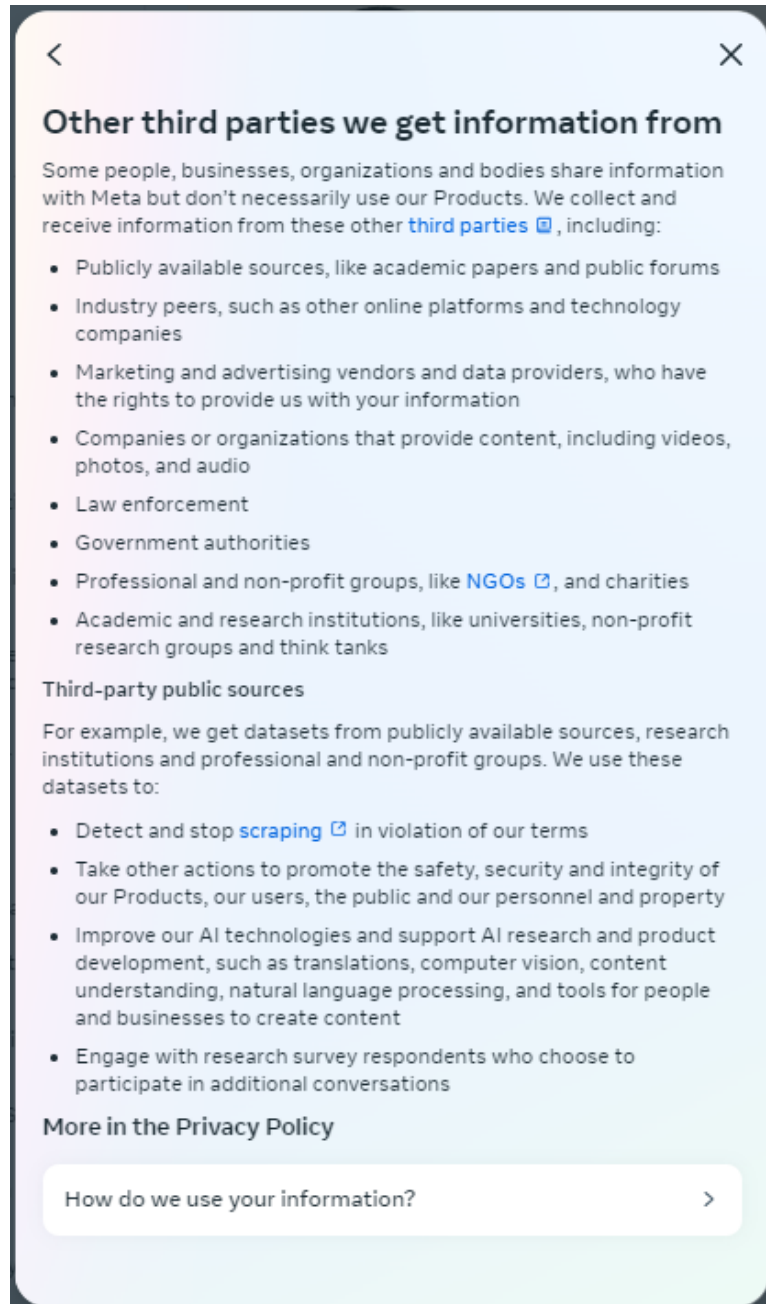
### How do we collect or receive this information from partners?

Partners use our [Business Tools](#) , integrations and Meta Audience Network technologies to share information with us.

These partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require partners to have the right to collect, use and share your information before giving it to us.

[Privacy Center](#)

125. Clicking on the “other third parties” link opens a new popup shown below<sup>38</sup> that indicates Meta receives audio from some companies or organizations that do not necessarily use Meta’s Products.



<sup>38</sup> Available at [https://www.facebook.com/privacy/policy?annotations\[0\]=1.ex.40-ThirdPartiesWeGet&subpage=1.subpage.4-InformationFromPartnersVendors](https://www.facebook.com/privacy/policy?annotations[0]=1.ex.40-ThirdPartiesWeGet&subpage=1.subpage.4-InformationFromPartnersVendors) (last visited Aug. 8, 2023).

126. Nothing in the Privacy Policy indicates that audio of a user sent by a third party may be used to create a voiceprint of a Facebook user or identify that user by comparing it to a voiceprint.

127. In sum, the Privacy Policy does not disclose that Meta creates, captures, collects, obtains, and utilizes voiceprints or related biometric information.

#### **D. Meta’s United States Regional Privacy Notice**

128. Near the top of the Privacy Policy is a sentence stating: “Read the United States Regional Privacy Notice for more details about how we handle Personal Information and how to exercise your rights.”<sup>39</sup>

#### **Privacy Policy**

#### **What is the Privacy Policy and what does it cover?**

Effective June 15, 2023 | [View printable version](#) | [See previous versions](#)

Read the [United States Regional Privacy Notice](#) [for more details about how we handle Personal Information and how to exercise your rights.](#)

129. The Privacy Policy does not indicate that the United States Regional Privacy Notice is applicable to all U.S. residents or that it contains supplemental terms to the Privacy Policy.

130. Prior to January 1, 2023, clicking on the link lead to a “California Privacy Notice,” which was applicable only to California residents.<sup>40</sup>

///

///

///

---

<sup>39</sup> Meta Privacy Policy, Effective June 15, 2023, <https://www.facebook.com/privacy/policy> (last visited Aug. 8, 2023).

<sup>40</sup> Available at <https://www.facebook.com/privacy/policies/uso/version/20220726/> (last visited Aug. 8, 2023).

131. As of January 1, 2023, clicking on the link in the Privacy Policy to “United States Regional Privacy Notice” (the “U.S. Privacy Notice”) reveals additional terms that “supplement[]” Meta’s Privacy Policy for all people living in the United States.<sup>41</sup>

### About this Notice

Effective January 1, 2023 | [View printable version](#) | [See previous versions](#)

This United States Regional Privacy Notice (“Notice”) is for people living in the United States and supplements the [Meta Privacy Policy](#), the [Meta Payments Inc. Privacy Policy](#), the [Meta Viewpoints Privacy Policy](#), the [Crowdtangle Data Policy](#), and the [Opensource Privacy Policy](#). For Portal, Facebook View, and Meta Platforms Technologies products, please see their [U.S. Regional Privacy Notice](#).

132. The U.S. Privacy Notice as updated on July 1, 2023. The provisions described herein are contained in both the January 2023 and July 2023 versions.

133. The U.S. Privacy Notice purports to explain how Meta collects, uses, and discloses Personal Information and “describes how to exercise your rights under” California, Colorado, Connecticut, Utah, and Virginia privacy laws.<sup>42</sup> There is no mention of Illinois law.

This Notice explains how we collect, use, and disclose your Personal Information. It also describes how to exercise your rights under the California Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act. We call those laws collectively the “U.S. Privacy Laws.”

134. The U.S. Privacy Notice explains that the term “Personal Information” means “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with you, directly or indirectly.”<sup>43</sup>

<sup>41</sup> U.S. Privacy Notice, Effective January 1, 2023, *available at* <https://www.facebook.com/privacy/policies/uso/version/5555449491171442/> (last visited Aug. 8, 2023).

<sup>42</sup> U.S. Privacy Notice, Effective July 1, 2023, <https://www.facebook.com/privacy/policies/uso/> (last visited Aug. 8, 2023).

<sup>43</sup> *Id.*



135. The U.S. Privacy Notice states that Meta “process[es] information about you, including Personal Information, whether or not you have an account or are logged in.”<sup>44</sup>

136. The U.S. Privacy Notice states that Meta “may disclose your Personal Information for business purposes . . . .”<sup>45</sup>

137. The U.S. Privacy Notice provides a “summary” of “[t]he categories of Personal Information we may have collected about you over the past 12 months,” “[h]ow we may use your Personal Information,” and “[t]o whom we may have disclosed that information.”<sup>46</sup>

138. The categories of Personal Information collected include, *inter alia*:

- Identifiers;
- Photos and videos, which may include face imagery;
- Internet or other electronic network activity information, including browser and app logs, content you view or engage with, and app, browser and device information;
- Location-related information; and
- Audio or visual information, including photos, videos, and voice recordings.<sup>47</sup>

139. The U.S. Privacy Notice continues, explaining that Meta may also collect additional “sensitive personal information” (as defined in the privacy laws of California, Colorado, Connecticut, Utah, and Virginia), including, *inter alia*:

---

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*



- Social security, driver's license, state identification card or passport number;
- The content of messages you send and receive;
- Information about your health; and
- Face imagery or *voice recordings which may be used to identify you when you use relevant features*.<sup>48</sup>

140. This is the first time Meta revealed in any of its communications directed to Meta users, albeit vaguely and not in compliance with BIPA, that it can use audio of voices to identify users.

141. A screenshot showing the statements quoted in paragraphs 137-139 is shown below:<sup>49</sup>

---

<sup>48</sup> *Id.* (emphasis added)

<sup>49</sup> *Id.*

The information we collect, use and disclose about you will vary depending on how you interact with Meta and our products. For the products covered by this Notice, here's a summary of:

- The categories of Personal Information we may have collected about you over the past 12 months
- How we may use your Personal Information
- To whom we may have disclosed that information

Categories of Personal Information we collect may include:	Examples of how Personal Information may be used include:	Parties with whom each category of Personal Information may be disclosed include:
<ul style="list-style-type: none"> <li>• Identifiers;</li> <li>• Characteristics of protected classifications;</li> <li>• Commercial information;</li> <li>• Photos and videos, which may include face imagery;</li> <li>• Internet or other electronic network activity information, including browser and app logs, content you view or engage with, and app, browser and device information;</li> <li>• Location-related information;</li> <li>• Audio or visual information, including photos, videos, and voice recordings;</li> <li>• Professional or employment information;</li> <li>• Education information;</li> <li>• Information derived from other Personal Information about you, which could include your preferences, interests, and other information used to personalize your experience; and</li> <li>• Other information you provide.</li> </ul> <p>We may also collect sensitive personal information (as defined in U.S. Privacy Laws), which may include:</p> <ul style="list-style-type: none"> <li>• Social security, driver's license, state identification card or passport number;</li> <li>• Precise geolocation;</li> <li>• Information about your racial or ethnic origin or religious views or union membership;</li> <li>• The content of messages you send and receive, which are considered sensitive personal information under CCPA;</li> <li>• Information about your sexual orientation;</li> <li>• Information about your health; and</li> <li>• Face imagery or voice recordings which may be used to identify you when you use relevant features.</li> </ul>	<ul style="list-style-type: none"> <li>• Providing, personalizing, and improving our products, including ads;</li> <li>• Providing measurement, analytics, and other business services;</li> <li>• Promoting safety, integrity, and security;</li> <li>• Providing marketing communications to you;</li> <li>• Communicating with you; and</li> <li>• Researching and innovating for social good.</li> </ul> <p>For categories of sensitive personal information that we collect, we will only use or disclose it either with your specific consent when required, or as otherwise permitted by law, including the CCPA. <a href="#">Learn more</a> about the permitted purposes under CCPA.</p>	<ul style="list-style-type: none"> <li>• People and accounts you share and communicate with;</li> <li>• People and accounts with which others share or reshare content about you;</li> <li>• Apps, websites, and third-party integrations on or using our products;</li> <li>• New owners in the event of a change of ownership or control of all or part of our products or their assets changes;</li> <li>• Partners, including partners offering goods and services on our products, as explained in our <a href="#">Privacy Policy</a> <a href="#">↗</a>;</li> <li>• Vendors, including measurement and marketing vendors;</li> <li>• Service providers;</li> <li>• Third parties, including external researchers and academics;</li> <li>• Law enforcement or other third parties in connection with legal requests, to comply with applicable law or to prevent harm; and</li> </ul> <p><a href="#">The Meta Companies</a>. <a href="#">↗</a></p>

142. Meta does not have a written retention schedule or guidelines for permanently destroying biometric identifiers and biometric information by the earlier of (a) when the initial purpose for collecting or obtaining them has been satisfied or (b) within 3 years of the person's last interaction with Meta.


143. Rather, as shown in the screenshot below, the U.S. Privacy Notice indicates that Meta will “keep Personal Information, including sensitive Personal Information, as long as we need it to provide our products, comply with legal obligations or protect our or other’s interests. We decide how long we need information on a case-by-case basis.”<sup>50</sup>

### How long do we keep your Personal Information?

We keep Personal Information, including sensitive Personal Information, as long as we need it to provide our products, comply with legal obligations or protect our or other’s interests. We decide how long we need information on a case-by-case basis.

Here’s what we consider when we decide:

- If we need it to operate or provide our products.
- The feature we use it for, and how that feature works.
- How long we need to retain the information to comply with certain legal obligations.
- If we need it for other legitimate purposes, such as to prevent harm; investigate possible violations of our terms or policies; promote safety, security and integrity; or protect ourselves, including our rights, property or products.

Learn more in the “Why we may preserve your information longer” section of the Meta Privacy Policy [here](#) .

144. The U.S. Privacy Notice does not seek any affirmative assent prior to obtaining voiceprints or related biometric data of Illinois residents.

145. Rather, as shown in the screenshot below, the U.S. Privacy Policy indicates opt-out requests and other actions a user must take to limit the use of biometric data (assuming he or she knows it is being collected).<sup>51</sup>

---

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

## How can you exercise your rights provided under the U.S. Privacy Laws?

Depending on where you live and subject to certain exceptions, you may have some or all of the following rights:

- **Right to Know:** The right to request that we disclose to you the Personal Information we collect, use, or disclose, and information about our data practices.
- **Right to Request Correction:** The right to request that we correct inaccurate Personal Information that we maintain about you.
- **Right to Request Deletion:** The right to request that we delete your Personal Information that we have collected from or about you.
- **Right to Opt Out of Targeted Advertising:** The right to opt out of the processing of your Personal Information obtained from your activities on nonaffiliated websites or online applications for the purposes of targeted advertising.
- **Right to Non-Discrimination:** The right not to receive discriminatory treatment for exercising your privacy rights.

To submit a request to exercise your rights, and as applicable, to appeal a consumer rights action, please visit this [webform](#).

To exercise the right to opt out of targeted advertising, see the "Activity information from ad partners" section in [Ad Preferences](#).

Please note that to protect your information and the integrity of our products, we may need to verify your identity before processing your request. In some cases, we may need to collect additional information to verify your identity, such as a government issued ID.

Under certain U.S. Privacy Laws, you may also designate an authorized agent to make these requests on your behalf. If you use an authorized agent to submit a request, we may need to collect additional information, such as a government issued ID, to verify your identity before processing your request to protect your information. In most cases, we will facilitate your request through automated tools available through your password-protected account.

For information on the CCPA requests we have received, please see [here](#).

146. BIPA, however, does not require Illinois residents to take action to stop or limit the collection and use of biometric data; rather, it requires Meta to obtain their informed consent and make other disclosures *before* it collects such data.

147. Meta's failures to comply with BIPA as set forth herein violated Plaintiff's and the Class Members' privacy rights, and the harm to Plaintiff and the Class occurred in Illinois. *See Cothron*, 477 F. Supp.3d at 732 n.7; *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547–48 (N.D. Cal. 2018).

## VI. Plaintiff's Experience

148. Plaintiff has a Facebook account and utilizes Meta's Messenger app.

149. On multiple occasions in 2023, 2022, and throughout the Class Period, Plaintiff has, for personal use, input her voice into an audio function on Facebook or Messenger,

1 including, *inter alia*, to dictate text messages to send via Messenger, sending an audio recording  
2 of her voice via Messenger, and making audio calls via Messenger.

3 150. Plaintiff believes that on other occasions during the Class Period, her voice has  
4 been captured by Meta via other users utilizing Facebook or Messenger and/or via third parties.

5 151. During the Class Period, Meta created, collected, captured, received through  
6 trade, stored, and/or otherwise obtained Plaintiff's voiceprint and related biometric information.

7 152. Meta did not receive a written release, executed by Plaintiff, before it created,  
8 collected, captured, received through trade, stored, and/or otherwise obtained Plaintiff's  
9 voiceprint and related biometric information.  
10

11 **CLASS ACTION ALLEGATIONS**

12 153. Plaintiff brings this class action on behalf of herself and all others similarly  
13 situated, as representative of the following class:

14 All natural persons in Illinois from whom Meta created, collected,  
15 captured, received, obtained, or stored Digital Voice Data, Voice  
16 Characteristics, and/or a Voice Profile.

17 154. Excluded from the Class is any Defendant, its parents, subsidiaries, affiliates,  
18 predecessors, successors, officers, directors, and the immediate family members of such persons.  
19 Also excluded are any trial judge who may preside over this action, court personnel and their  
20 family members and any juror assigned to this action.

21 155. Plaintiff is a member of the Class she seeks to represent.

22 156. Plaintiff reserves the right to amend or modify the Class definitions with greater  
23 specificity or division into subclasses after having had an opportunity to conduct discovery.

24 157. The Class Period is that period within the statute of limitations for this action and  
25 extending until a Class is certified herein.

26 158. The Class is certifiable under Fed. R. Civ. P. 23.  
27  
28

159. **Numerosity.** The members of the Class are so numerous that joinder of all members is impracticable. The determination of the numerosity factor can be made from Defendant's records.

160. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members have had their rights under BIPA violated based on Meta's failure to comply with the provisions of BIPA.

161. **Commonality and Predominance.** There are questions of law and fact common to the Class, which predominate over any questions affecting individual members of the Class. These common questions of law and fact include, without limitation:

- a. Whether Meta possessed, created, collected, captured, received through trade, stored, or otherwise obtained biometric identifiers or biometric information of Plaintiff and the Class;
- b. Whether Meta developed, made available to the public, and complied with a retention and destruction policy in compliance with 740 ILCS 14/15(a);
- c. Whether Meta informed Plaintiff and the Class in writing that it was collecting their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(1);
- d. Whether Meta informed Plaintiff and the Class in writing of the specific purpose and length of term for which it was collecting their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(2);
- e. Whether Meta received written releases executed by Plaintiff and the Class before capturing, collecting, receiving through trade, or

otherwise obtaining their biometric identifiers or biometric information in compliance with 740 ILCS 14/15(b)(3);

f. Whether Meta sold, leased, traded, or otherwise profited from the biometric identifiers or biometric information of Plaintiff and the Class;

g. Whether Meta stored, transmitted, and protected from disclosure all biometric identifiers and biometric information of Plaintiff and the Class using the reasonable standard of care within the industry in compliance with 740 ILCS 14/15(e)(1);

h. Whether Meta stored, transmitted, and protected from disclosure all biometric identifiers and biometric information of Plaintiff and the Class in a manner that is the same as or more protective than the manner in which it stores, transmits, and protects other confidential and sensitive information in compliance with 740 ILCS 14/15(e)(2); and/or

i. Whether any violations of BIPA by Meta were reckless, intentional, or negligent.

162. **Adequacy.** Plaintiff is a member of the Class she seeks to represent, is committed to the vigorous prosecution of this action, and has retained competent counsel experienced in the prosecution of class actions. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

163. **Superiority.** A class action is an appropriate method for the fair and efficient adjudication of this controversy and is superior to all other available methods. Because the amount of each individual Class member's claim is small relative to the complexity of the



litigation, and due to the financial resources of Defendant, no Class member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, Class members will continue to suffer harm and Defendant's misconduct will proceed without remedy. Even if Class members could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard that might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court. Finally, Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

164. **Class Action on Limited Issues.** Because there are common individual issues among the Class, it is appropriate for this action to be maintained as a class action with respect to particular issues if necessary. *See* Fed. R. Civ. P. 23(c)(4).

## **CLAIMS FOR RELIEF**

### **COUNT I**

#### **Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(a)**

165. Plaintiff incorporates by reference each and every allegation set forth above.

166. Meta is a "private entity" under BIPA. 740 ILCS 14/10.

167. During the Class Period, Meta has been in possession of the voiceprints and related biometric information of Plaintiff and the Class.

168. During the Class Period, Meta did not develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric



1 identifiers and biometric information to occur by the earlier of: (a) when the original purpose for  
2 collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's  
3 last interaction with the private entity, as required by 740 ILCS 14/15(a).

4 169. Instead, Meta's stated policy was that it would retain any data it collected,  
5 including sensitive personal information, "as long as we need it to provide our products, comply  
6 with legal obligations or protect our or other's interests" and that "[w]e decide how long we need  
7 information."

8 170. Thus, Meta has failed to comply with a retention/destruction policy that conforms  
9 to BIPA § 15(a) and has unlawfully retained biometric identifiers and biometric information of  
10 Plaintiff and the Class.

11 171. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act,  
12 recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

13 172. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's  
14 violation of their rights under BIPA, and accordingly are entitled to seek damages and relief  
15 provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

16 173. Meta's failure to maintain and comply with data retention and destruction  
17 protocols harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff  
18 and the Class, including the right to make informed choices about the use of and control over  
19 their inherently sensitive biometric data and to be free from unlawful retention of such sensitive  
20 data.

21 174. Plaintiff and the Class Members seek, *inter alia*, statutory damages of \$5,000 per  
22 intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of  
23 \$1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys'  
24 fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

## **COUNT II**

### **Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(b)**

175. Plaintiff incorporates by reference each and every allegation set forth above.

176. During the Class Period, Meta collected, captured, received through trade, and/or otherwise obtained the voiceprints and related biometric information of Plaintiff and the Class.

177. Plaintiff and the Class did not execute a written release related to Meta's collection, capturing, purchasing, receiving through trade, or otherwise obtaining their voiceprints or related biometric information.

178. During the Class Period, Meta did not properly inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information was being collected and/or stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

179. During the Class Period, Meta systematically and intentionally collected, obtained, used, and/or stored the biometric identifiers and/or biometric information of Plaintiff and the Class without first obtaining from Plaintiff and the Class Members the specific executed written release required by 740 ILCS 14/15(b)(3).

180. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act, recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

181. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

182. Meta's failure to disclose its practices and obtain the informed consent of Plaintiff and the Class Members before collecting, capturing, receiving through trade, and/or otherwise obtaining their biometric data harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data and to be free from the unlawful collection of such sensitive data.

183. Plaintiff and the Class Members seek, *inter alia*, statutory damages of \$5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of \$1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

### **COUNT III**

#### **Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(c)**

184. Plaintiff incorporates by reference each and every allegation set forth above.

185. As set forth above, during the Class Period, Meta used the biometric identifiers and/or biometric information of Plaintiff and the Class that was in its possession to improve Meta's natural language understanding, machine learning, and for its own commercial purposes.

186. Meta's use of the biometric identifiers and biometric information of Plaintiff and the Class to improve Meta's natural language understanding and machine learning, expand the scope of Meta's products, provide targeted content and advertising, and create other business opportunities for Meta has allowed Meta to profit through increased sales of its improved voice-recognition products and services that utilize voice-recognition, and increased targeting of its advertisements for which it receives most of its annual revenue.

1 187. Moreover, Meta has profited from linking the voiceprints in its possession to  
2 Plaintiff and the Class's Facebook profiles and other activities involving Meta.

3 188. Furthermore, Meta has used the biometric identifiers and biometric information  
4 of Plaintiff and the Class to create technology that is so intertwined with the biometric data that  
5 marketing the Meta voice-recognition technology and targeted content that utilizes it is  
6 essentially disseminating biometric data for profit.

7 189. Additionally, Meta has used the biometric identifiers and biometric information  
8 of Plaintiff and the Class to obtain a competitive advantage over other businesses offering similar  
9 devices that provide similar voice-based services and targeted advertising as Meta.

10 190. Accordingly, Meta violated 740 ILCS 14/15(c) by selling, leasing, trading, or  
11 otherwise profiting from Plaintiff's and Class Members' biometric identifiers and/or biometric  
12 information in its possession.

13 191. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act,  
14 recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

15 192. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's  
16 violation of their rights under BIPA, and accordingly are entitled to seek damages and relief  
17 provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

18 193. Meta's selling, leasing, trading, or otherwise profiting from Plaintiff's and Class  
19 Members' biometric identifiers and/or biometric information in its possession harmed, or posed  
20 a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the  
21 right to manage the collection of, use of, and control over inherently sensitive biometric data in  
22 the possession of others.

23 194. Plaintiff and the Class Members seek, *inter alia*, statutory damages of \$5,000 per  
24 intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of  
25

1 \$1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys'  
 2 fees and costs pursuant to 740 ILCS 14/20(3).

3 WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for  
 4 Relief set forth below.

#### 5 **COUNT IV**

##### 6 **Meta's Violations of the Biometric Information Privacy Act, 740 ILCS 14/15(e)**

7 195. Plaintiff incorporates by reference each and every allegation set forth above.

8 196. During the Class Period, Meta has failed to store, transmit, and protect from  
 9 disclosure the biometric identifiers and/or biometric information of Plaintiff and the Class using  
 10 the reasonable standard of care within the industry, in violation of 740 ILCS 14/15(e)(1).

11 197. Additionally, during the Class Period, Meta has failed to store, transmit, and  
 12 protect from disclosure the biometric identifiers and/or biometric information of Plaintiff and the  
 13 Class in a manner that is the same as or more protective than the manner in which the private  
 14 entity stores, transmits, and protects other confidential and sensitive information.

15 198. For example, as set forth above, Meta acknowledges that its large size and vast  
 16 amount of user data makes it a key target for cyber-attacks, has disclosed it has been the subject  
 17 of cyber-attacks in the past, states it will be subject to future intrusions, and admits it may not be  
 18 aware of or discover all such intrusions.

19 199. In violating BIPA, a law in effect since 2008, Meta acted, and continues to act,  
 20 recklessly and/or intentionally. At the least, Meta negligently violated BIPA.

21 200. Plaintiff and the Class Members are "aggrieved" under BIPA based on Meta's  
 22 violation of their rights under BIPA, and accordingly are entitled to seek damages and relief  
 23 provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

201. Meta's failure to properly store the biometric data of Plaintiff and the Class Members harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Class, including the right to manage the storage of, and control over, inherently sensitive biometric data in the possession of others.

202. Plaintiff and the Class Members seek, *inter alia*, statutory damages of \$5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), statutory damages of \$1,000 per negligent violation of BIPA pursuant to 740 ILCS 14/20(1), and reasonable attorneys' fees and costs pursuant to 740 ILCS 14/20(3).

WHEREFORE, Plaintiff and the Class pray for the relief requested in the Prayer for Relief set forth below.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and the Class, pray for judgment against Defendant as follows:

A. entering an order certifying the Class and appointing Plaintiff as their representative as requested herein, and appointing the undersigned as counsel for the Class;

B. awarding statutory damages of \$5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, in the alternative, statutory damages of \$1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

C. enjoining Meta from creating, collecting, obtaining, storing, using, selling, leasing, trading, and profiting from Plaintiff's and the Class's biometric identifiers and biometric information until done so in compliance with BIPA;

D. awarding Plaintiff reasonable attorneys' fees, costs, and other expenses pursuant to 740 ILCS 14/20(3);

1 E. awarding Plaintiff pre-judgment and post-judgment interest, as provided  
2 by law; and

3 F. awarding such other and further relief as is just and appropriate.  
4

5 Dated: August 16, 2023

**ARIAS SANGUINETTI WANG & TORRIJOS LLP**

7 By: /s/ Mike Arias

8 MIKE ARIAS  
9 ELISE R. SANGUINETTI  
10 ARNOLD C. WANG  
11 CRAIG S. MOMITA  
12 M. ANTHONY JENKINS

**GOLDENBERG HELLER & ANTOGNOLI, P.C.**

13 THOMAS P. ROSENFELD  
14 KEVIN P. GREEN  
15 THOMAS C. HORSCROFT

Attorneys for Plaintiff

**JURY DEMAND**

16 Plaintiff demands a trial by jury on all claims so triable.

17 Dated: August 16, 2023

**ARIAS SANGUINETTI WANG & TORRIJOS LLP**

19 By: /s/ Mike Arias

20 MIKE ARIAS  
21 ELISE R. SANGUINETTI  
22 ARNOLD C. WANG  
23 CRAIG S. MOMITA  
24 M. ANTHONY JENKINS

**GOLDENBERG HELLER & ANTOGNOLI, P.C.**

25 THOMAS P. ROSENFELD  
26 KEVIN P. GREEN  
27 THOMAS C. HORSCROFT

Attorneys for Plaintiff